
 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 1 de 28

## Tabla de contenido

1. Objetivos .....	2
2. Alcance .....	2
3. Glosario .....	3
4. Marco normativo .....	3
5. Desarrollo .....	3
5.1 Contexto estratégico .....	4
5.2 Identificación de riesgos .....	5
5.3 Valoración de riesgos .....	7
5.4 Tratamiento de los riesgos .....	10
5.5 Monitoreo, revisión y evaluación del riesgo .....	11
5.6 Tratamiento de riesgos materializados .....	12
6. Responsabilidades y competencias .....	14
7. Evaluación del lineamiento.....	15
8. Administración del lineamiento.....	16
9. Aprobación del documento.....	17

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 2 de 28

## 1. Objetivos

Establecer las directrices para la administración de riesgos en la Secretaría Distrital de Integración Social - SDIS, a través de la armonización de los lineamientos y la normativa vigente en la materia, con el fin de garantizar la adecuada identificación y tratamiento de los riesgos asociados a los procesos de la entidad, en cumplimiento de la misión institucional y objetivos estratégicos.

### Objetivos específicos

- Definir los criterios para identificar y gestionar los riesgos asociados a los procesos de la entidad.
- Definir los criterios para establecer actividades de control preventivas, detectivas y correctivas para los riesgos identificados, con el fin de mitigar los posibles efectos de su materialización en el cumplimiento de las disposiciones legales, la misión institucional y los objetivos estratégicos.
- Definir los criterios para actuar de manera oportuna ante la materialización de los riesgos identificados.

## 2. Alcance


El lineamiento o Política de Administración de Riesgos<sup>1</sup> de la Secretaría Distrital de Integración Social abarca el manejo de los riesgos asociados a los procesos definidos por la entidad, incluyendo los correspondientes a gestión, seguridad de la información y corrupción, teniendo en cuenta las consideraciones particulares que se señalen en el numeral 5 de este lineamiento y en las demás directrices oficiales derivadas del mismo. Así mismo, considera que, dentro de los riesgos de gestión o corrupción se podrán identificar riesgos fiscales y a su vez dentro de los riesgos de corrupción se incluirán los riesgos identificados del Lavado de Activos, Financiación del Terrorismo o Financiación de la Proliferación de armas de destrucción masiva - LA/FT/FP<sup>2</sup>.

Los riesgos de gestión identificados para los procesos podrán considerar los planes, programas o proyectos que contribuyan al cumplimiento de los objetivos institucionales.

Respecto a los riesgos asociados a los sistemas de gestión que implemente la entidad (riesgos laborales, riesgos en la gestión documental, riesgos derivados de los aspectos e impactos ambientales, riesgos de interrupción, entre otros), su administración se llevará a cabo de conformidad con las directrices específicas que genere cada sistema. En el momento en que

<sup>1</sup> Política de administración de riesgos: declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (DAFP, 2022). Para la Secretaría Distrital de Integración Social, el Lineamiento Administración de riesgos, corresponde a la política interna de operación en esta materia.

<sup>2</sup> Riesgo de Lavado de Activos y Financiación del Terrorismo – LA/FT: se define como la posibilidad de pérdida o daño que puede sufrir una entidad por su propensión a ser utilizada directamente o a través de sus operaciones, como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades. Documento Técnico, Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital (Secretaría General, diciembre de 2022).

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 3 de 28

tales riesgos se articulen en su metodología de valoración a lo referido en este lineamiento, podrán armonizarse bajo el mismo instrumento.

### 3. Glosario

Los términos y definiciones aplicables al documento pueden ser consultados en el glosario institucional en el Manual del Sistema de Gestión / Novedades / Glosario Institucional: <https://sig.sdis.gov.co/index.php/es/novedades/glosario-institucional>.

### 4. Marco normativo


- Decreto 1499 de 2017 “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”, artículo 2.2.22.3.5.
- CONPES 3995 del 1 de julio de 2020, Política Nacional de confianza y seguridad digital.
- Decreto Distrital 221 de 2023 “Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital, se deroga el Decreto Distrital 807 de 2019 y se dictan otras disposiciones”.
- Resolución interna No. 1375 de 2023 de la Secretaría Distrital de Integración Social “Por la cual se reglamenta el Comité Institucional de Coordinación de Control Interno en la Secretaría Distrital de Integración Social, y se deroga la Resolución No. 0525 del 17 de abril de 2018”, artículo 3, literales g y h.
- Modelo de Gestión de Riesgos de Seguridad Digital<sup>3</sup> (MGRSD).
- Circular 092 de 2020 de la Secretaría General de la Alcaldía Mayor de Bogotá “Implementación del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo -SARLAFT en las entidades distritales”.

### 5. Desarrollo

El lineamiento de administración de riesgos se rige por los conceptos y directrices de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública - DAFP<sup>4</sup>.

<sup>3</sup> Ministerio de Tecnologías de la Información y las Comunicaciones.  
<https://www.urnadecristal.gov.co/sites/default/files/MODELO%20DE%20GESTI%C3%93N%20DE%20RIESGOS%20DE%20SEGURIDAD%20DIGITAL.PDF>

<sup>4</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 4 de 28

Los riesgos en la Secretaría Distrital de Integración Social se categorizan por procesos, entendiendo que, si en el marco de los planes, programas o proyectos se identifican riesgos, éstos se gestionarán de acuerdo con las directrices o metodologías que establezcan su existencia y podrán considerarse como insumos para la identificación o actualización de riesgos estratégicos que se deberán enmarcar dentro de los procesos institucionales. En este sentido, es importante tener en cuenta que al tomar como insumo de referencia los riesgos asociados a los proyectos de inversión, así como aquellos que se derivan de los sistemas de gestión que implemente la entidad (riesgos laborales, riesgos en la gestión documental, riesgos derivados de los aspectos e impactos ambientales, riesgos de interrupción, riesgos LA/FT/FP, entre otros), el proceso estará integrando elementos estratégicos para el cumplimiento de los objetivos institucionales.


Los riesgos de seguridad de la información identificados deberán alinearse con los objetivos y controles definidos en la política de seguridad y privacidad de la información de la entidad, conforme a la norma ISO/IEC 27001:2022. Por su parte, los riesgos que se lleguen a identificar, asociados a tecnologías emergentes como inteligencia artificial, servicios en la nube, dispositivos IoT y big data, deberán ser evaluados al menos una vez al año, o cuando se adopte un nuevo servicio digital.

La política de administración de riesgos se opera a través del procedimiento Administración de riesgos (PCD-SG-003), que incorpora las directrices de la guía de administración del riesgo del DAFP en las etapas de contexto estratégico, identificación, valoración, monitoreo y revisión.

## 5.1 Contexto estratégico

Es la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. A partir de los factores que se definan, es posible establecer las causas de los riesgos a identificar. En concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión - MIPG, esta actividad corresponde al equipo directivo y se realizará desde el proceso Planeación estratégica, como marco general dentro del cual se realizará el análisis de los equipos operativos.

Para el establecimiento del contexto externo se determinan las características o aspectos esenciales del entorno en el cual opera la entidad y se pueden considerar factores políticos, económicos, financieros y presupuestales, sociales y culturales, fiscales, tecnológicos, ambientales, reputacionales, legales y reglamentarios, o de exposición institucional a eventos de fraude. Por su parte, para el establecimiento del contexto interno, se determinan las características o aspectos esenciales del ambiente en el cual la entidad busca alcanzar sus objetivos y se pueden considerar factores como: estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias implementadas, recursos y conocimientos con que se cuenta (personas, procesos, sistemas, tecnología), relaciones con las partes involucradas, cultura organizacional, resultados de los seguimientos y auditorías producto de la evaluación de la Oficina de Control Interno, resultados de las evaluaciones realizadas por entes

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 5 de 28

de control, resultados de seguimiento a las Peticiones, Quejas, Reclamos, Sugerencias y Denuncias-PQRSD, y recomendaciones del Comité Institucional de Gestión y Desempeño.

Adicionalmente, corresponde a la Dirección de Análisis y Diseño Estratégico realizar un análisis de los objetivos de la entidad, tanto del orden estratégico como de procesos, revisando que se encuentren alineados con la Misión y la Visión Institucional, y asegurando que los objetivos de proceso contribuyen a los objetivos estratégicos. Este análisis se realizará por lo menos cada cuatro años a partir de la actualización de la plataforma estratégica verificando que los objetivos sean medibles, realistas y que expresen una acción descrita con un verbo fuerte.

De esta manera, los equipos operativos podrán establecer el contexto del proceso en el cual se determinen las características o aspectos esenciales del mismo y sus interrelaciones. Se pueden considerar factores como: objetivo del proceso, alcance del proceso, interrelación con otros procesos, procedimientos asociados, responsables del proceso y activos de información asociados al proceso.

Por su parte, como primer paso para la identificación de riesgos de seguridad de la información es necesario contar con una identificación de los activos de información asociados a cada uno de los procesos de la entidad, lo cual permite definir qué es lo más crítico para la entidad en cuanto a confidencialidad, integridad y disponibilidad de la información (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

La identificación y valoración de los activos de información debe ser realizada por la Primera Línea – Líderes de Proceso, en cada proceso, siendo debidamente orientados por el Líder de gestión documental y el Oficial de seguridad de la información de la entidad o quien haga sus veces en la Subdirección de Investigación e Información.


Respecto al Sistema de Administración de Riesgos de Lavado de Activos y la Financiación del Terrorismo, en adelante SARLAFT, como primera instancia se cuenta con lo manifestado en las directrices de prevención LA/FT/FP de la entidad, que se emitan desde la Subsecretaría de Gestión Institucional, en las cuales se incluye el objetivo, alcance y metodología para la identificación de estos eventos. Los riesgos identificados de esta tipología serán gestionados con lo establecido en este Lineamiento para los riesgos de corrupción.

## 5.2 Identificación de riesgos

La identificación del riesgo de gestión se lleva a cabo con base en el contexto interno, externo y los objetivos del proceso, aplicando los siguientes pasos<sup>5</sup>:

- Identificación de los puntos de riesgo: son las actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

<sup>5</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 6 de 28

- Identificación de áreas de factores de riesgo: son las fuentes generadoras de riesgos. Algunos factores pueden ser: procesos, talento humano, tecnología, infraestructura o eventos externos, entre otros.
- Descripción del riesgo: la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso.
- Identificación de áreas de impacto: el área de impacto es la consecuencia económica (o presupuestal) y reputacional, a la cual se ve expuesta la entidad en caso de materializarse un riesgo.
- Clasificación del riesgo: son las categorías que permiten agrupar los riesgos identificados, en relación con los factores de riesgo.

Por su parte, al identificar riesgos de corrupción es importante que en la descripción concurren todos los componentes de su definición, es decir: acción u omisión + uso del poder + desviación de la gestión de lo público + beneficio privado. En el [anexo 1](#) se relacionan sugerencias de riesgos de corrupción que pueden ser consideradas en los análisis en los diferentes procesos. Así mismo, en el [anexo 3](#), se presentan ejemplos de situaciones que activan señales de alerta a partir de las cuales los procesos podrán identificar riesgos de lavado de activos, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.


Dentro de los riesgos de gestión y corrupción, se podrán identificar riesgos fiscales. En este sentido, en el [anexo 2](#) se presentan las *Circunstancias Inmediatas* más comunes en la gestión pública, que se derivan de los *Puntos de Riesgo Fiscal*, que han sido identificados por el Departamento Administrativo de la Función Pública, a partir del análisis de fallos con responsabilidad fiscal de la Contraloría General de la Republica y de las Contralorías territoriales<sup>6</sup>.

Finalmente, los riesgos de seguridad de la información, que incluyen a su vez los riesgos de seguridad digital, se tipifican como la:

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

La seguridad de la información abarca varios ítems relacionados entre sí, como lo son la continuidad del negocio, las tecnologías de la información y la ciberseguridad; por lo cual, la gestión del riesgo es una labor que debe ser afrontada de manera integral. En este contexto, la identificación de riesgos asociados a la protección de datos personales es importante para la Secretaría Distrital de Integración Social debido a que en el cumplimiento de su misionalidad recolecta, recibe y transfiere, datos personales.

<sup>6</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022. Anexo 6.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 7 de 28

Para cada riesgo de seguridad de la información 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.

Amenazas comunes:

En el [anexo 4](#), se presenta la lista que indica cada tipo de amenaza donde D (deliberada), A (accidental), E (entorno). En este sentido, D se utiliza para todas las acciones deliberadas dirigidas a los activos de información, A se utiliza para todas las acciones humanas que pueden dañar accidentalmente los activos de información, y E se utiliza para todos los incidentes que no se basan en acciones humanas. Los grupos de amenazas no están en orden de prioridad.

5.3 Valoración de riesgos

La valoración 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 el nivel de exposición final (riesgo residual). Esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas tomando relevancia el enfoque basado en riesgos que permita la toma de decisiones respecto a los impactos que se puedan presentar, atendiendo a la recomendación número 1 del Grupo de Acción Financiera Internacional y 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”.


5.3.1 Análisis y evaluación de riesgos

El análisis busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo inicial (riesgo inherente) y las acciones que se van a implementar. En el análisis del riesgo 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 servidores de la entidad.

La calificación de la probabilidad se asocia a la exposición que la actividad del proceso tenga al riesgo. De esta manera, la probabilidad corresponde a la frecuencia con que la actividad (punto de riesgo) se ejecuta en un (1) año. Los criterios para definir el nivel de probabilidad son:

Probabilidad	
Muy baja	20%
Baja	40%
Media	60%
Alta	80%
Muy alta	100%

Al calificar el impacto, se considera que las diferentes consecuencias o afectaciones se agrupan en lo económico y lo reputacional, por lo cual el análisis de los líderes de proceso con sus

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 8 de 28

equipos, se enfoca en las afectaciones bajo estos dos aspectos. Los criterios para definir el nivel de impacto son:

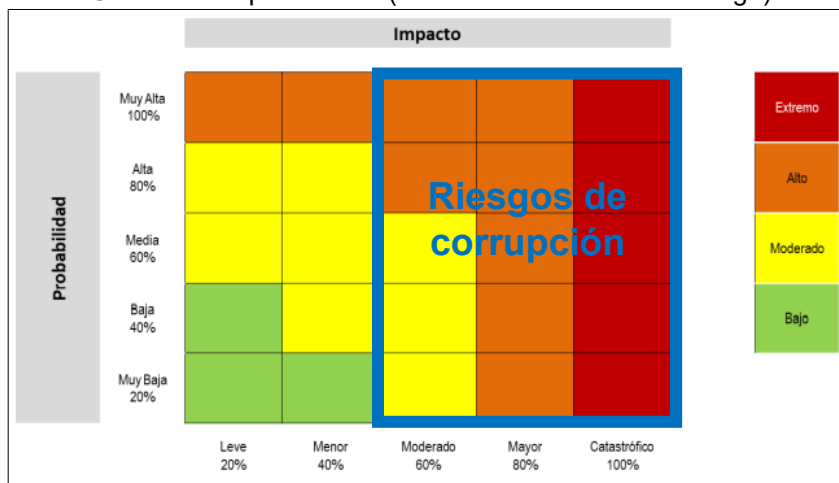
Impacto	
Leve	20%
Menor	40%
Moderado	60%
Mayor	80%
Catastrófico	100%

Para el caso de los riesgos de corrupción, el impacto siempre será negativo; por tanto, la calificación de impacto menor o leve no aplica para la evaluación del riesgo. El impacto para los riesgos de corrupción se calificará así:

Impacto	
Moderado	60%
Mayor	80%
Catastrófico	100%


La evaluación del riesgo se determina combinando la probabilidad con el impacto en el mapa de calor (gráfica 1), dando como resultado el nivel donde se encuentra el riesgo:

Gráfica 1: Mapa de calor (niveles de severidad del riesgo)



Fuente: "Guía para la administración del riesgo y el diseño de controles en entidades públicas" DAFF. Versión 6. Año 2022.

Para el caso en que el análisis y evaluación del riesgo inherente dé como resultado un nivel de exposición bajo (color verde), el líder del proceso podrá tomar la decisión de asumir el riesgo y de esta manera no se deberá continuar con el desarrollo de la metodología (apetito de riesgo). No obstante, los riesgos de corrupción ubicados en cualquier nivel de exposición deberán ser administrados.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 9 de 28

### 5.3.2 Estructura para el diseño de controles

Al momento de definir las actividades de control<sup>7</sup> se debe validar que estas mitigan el riesgo, para lo cual en su diseño se debe mantener la siguiente estructura y variables<sup>8</sup>:

1. **Responsable de ejecutar el control:** se debe precisar un cargo o rol específico, evitando hacer referencia a grupos de trabajo o áreas de manera general. No obstante, el responsable de coordinar y asegurar el cumplimiento del control será siempre el líder del proceso. En caso de que sean controles automáticos se debe relacionar el nombre del sistema que realiza la actividad.
2. **Acción:** se debe describir cómo se realiza la actividad de control e indicar cuál es su propósito, precisando para qué se realiza la actividad, considerando acciones como verificar, validar, cotejar, comparar o revisar, entre otras. Esta acción debe ser ejecutada por lo menos una vez dentro del periodo para la ejecución del plan de tratamiento y debe permitir identificar si el control se encuentra documentado.
3. **Complemento:** corresponde a los detalles que permitan identificar otros atributos del control. Estos deben incluir:
  - a. Frecuencia definida para su ejecución. Debe ser permanente y oportuna para mitigar el riesgo, de acuerdo con la naturaleza de la actividad y los recursos disponibles.
  - b. Evidencia de la ejecución del control. Debe permitir que, al ser revisada por un tercero, éste tenga las mismas conclusiones que el responsable de la ejecución. Debe permitir evaluar si la fuente de la información que sirve para ejecutar el control es confiable.
  - c. Documentación. Indique si el control se encuentra documentado en algún documento del Sistema de Gestión, documento administrativo, instrumento institucional o acto administrativo.

El líder del proceso, a partir de la metodología e instrumentos definidos por la Dirección de Análisis y Diseño Estratégico y la Subdirección de Diseño, Evaluación y Sistematización, debe asegurar que las actividades de control se encuentran bien diseñadas y que estas se ejecutan tal como han sido definidas, lo cual será revisado mediante las actividades de validación que ésta realiza como segunda línea, y mediante las acciones de auditoría interna o evaluación independiente realizadas por la Oficina de Control Interno (tercera línea).


Las actividades de control se clasifican como<sup>9</sup>:

- **Preventivas:** están diseñadas para evitar un evento no deseado antes del momento en que se produzca. Este tipo de controles se activan en la entrada del proceso y antes de que se ejecute la actividad que puede dar origen al riesgo, y se dirigen a las causas del mismo

<sup>7</sup> Control: medida que permite reducir o mitigar un riesgo. Para efectos del presente documento, al referenciar “control” se entenderá como las actividades establecidas a través de políticas, procedimientos u otras directrices, que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos institucionales.

<sup>8</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

<sup>9</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 10 de 28

atacando la probabilidad de ocurrencia, buscando establecer las condiciones que aseguren el resultado final esperado.


- **Detectivas:** estos controles buscan detectar la situación no deseada durante la ejecución del proceso o actividad originadora, para que se corrija y se tomen las acciones correspondientes.
- **Correctivas:** se diseñan para atacar el impacto generado por la materialización de un riesgo. Estos controles se activan en la salida del proceso o actividad originadora, después de que se materializa el riesgo, por lo cual los mismos no serán considerados en el plan de tratamiento (que tiene una naturaleza preventiva), sino que serán diseñados y ejecutados en el marco de los planes de restablecimiento.

Las actividades de control preventivas y detectivas deben ser evaluadas en su diseño y ejecución con el propósito de establecer la medida en la cual el control resulta adecuado para la mitigación del riesgo. La forma en que estas actividades de control afectan la probabilidad y/o el impacto determina la ubicación final del riesgo en el mapa de calor (Gráfica 1), lo cual se conoce como riesgo residual.

#### 5.4 Tratamiento de los riesgos

Luego de valorar el riesgo, el líder del proceso debe decidir si reduce, acepta o evita el riesgo, de la siguiente manera:

- **Reducir:** Implica tomar medidas encaminadas a disminuir el nivel de severidad del riesgo. Una opción es “mitigar”, lo cual se consigue generalmente mediante la optimización de los procedimientos y la implementación de acciones que no necesariamente sean adicionales a los controles ya establecidos. Otra opción es “transferir”, lo cual se consigue mediante la tercerización de procesos o el traslado del riesgo a través de seguros o pólizas con los cuales se hace un traspaso de las pérdidas a otras organizaciones.
- **Aceptar:** Es una medida en la cual se asume el riesgo conociendo los efectos de su posible materialización. Para la Secretaría Distrital de Integración Social, solamente es aplicable a los riesgos en zona baja o para aquellos a los cuales no se les pueda aplicar controles, sin embargo, en cualquier caso debe existir un seguimiento continuo del riesgo. Esta alternativa de tratamiento no es permitida en ningún caso para los riesgos de corrupción que se identifiquen.
- **Evitar:** En esta estrategia se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad originadora. Al ser una medida en la cual se elimina el riesgo en su totalidad, es un tratamiento simple, pero obstaculiza el cumplimiento de la misión de la entidad, por lo cual en la mayoría de los casos no es una opción viable.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 11 de 28

De esta manera se establecen los niveles de aceptación del riesgo residual así:

- Para los riesgos ubicados en el **nivel de exposición bajo** se asumirá el riesgo y los líderes de proceso realizarán monitoreo y reporte trimestral con el fin de validar que la calificación de probabilidad e impacto no ha tenido cambios, y que las actividades de control se ejecutan de acuerdo con lo programado.
- Para los riesgos ubicados en los **niveles de exposición moderado, alto y extremo** se adoptarán medidas para evitar o reducir el riesgo, de tal manera que se formularán actividades de control sobre las cuales los líderes de proceso realizarán monitoreo trimestral y reporte.
- Para los riesgos de corrupción ubicados en cualquier nivel de exposición se adoptarán medidas para evitar, reducir o compartir el riesgo, de tal manera que se formularán actividades de control sobre las cuales los líderes de proceso realizarán monitoreo y reporte trimestral.

De esta manera el plan de tratamiento del riesgo corresponderá a las actividades de control establecidas por la primera línea, para la mitigación de los diferentes riesgos.


### 5.5 Monitoreo, revisión y evaluación del riesgo

Es el paso que asegura el logro de los objetivos institucionales mediante la previsión de los eventos negativos asociados a la gestión de la entidad y se desarrolla a través de un esquema de asignación de responsabilidades y roles (ver numeral 9. “Responsabilidades y competencias”) de la siguiente manera:

- Primera línea: desarrolla e implementa procesos de autocontrol y gestión de riesgos a través de su identificación, análisis, valoración y monitoreo.
- Segunda línea: revisa que las actividades de control y los procesos de gestión de riesgos implementados por la primera línea, estén diseñados apropiadamente y funcionen como se pretende.
- Tercera línea: evalúa de manera independiente la gestión de riesgos institucional incluyendo la operación de la primera y segunda línea, con el fin de aportar información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos.

A partir de lo anterior, el monitoreo y revisión del riesgo tiene cuatro componentes:

- I. Trimestralmente los líderes de proceso (1ª línea) deberán realizar monitoreo a las actividades de control formuladas realizando el registro y reporte de los avances a la Dirección de Análisis y Diseño Estratégico-Subdirección de Diseño, Evaluación y Sistematización (2ª línea) conforme a lo dispuesto en el procedimiento Administración de riesgos vigente.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 12 de 28

Adicionalmente, los líderes de los procesos en conjunto con sus equipos deben revisar periódicamente sus mapas de riesgos, y si es el caso actualizarlos, presentando a la segunda línea la justificación técnica que sustente el ajuste requerido. Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos.

Este monitoreo también permitirá detectar los riesgos materializados.

- II. Trimestralmente, la Dirección de Análisis y Diseño Estratégico y/o sus Subdirecciones (2ª línea, según corresponda) deberán revisar las actividades de gestión del riesgo y control ejecutadas por la primera línea, informando las observaciones pertinentes respecto a lo reportado con el fin de fortalecer el cumplimiento de las etapas de administración de riesgos.
- III. Anualmente, la Dirección de Análisis y Diseño Estratégico-Subdirección de Diseño, Evaluación y Sistematización (2ª línea) deberá remitir a la Oficina de Control Interno (3ª línea), el resultado de la revisión realizada como segunda línea.

Una vez recibidos los resultados presentados por la segunda línea, de acuerdo con lo definido en el Plan Anual de Auditoría aprobado para cada vigencia, la Oficina de Control Interno evaluará la gestión de riesgos institucional, verificando el cumplimiento propio de los objetivos de la administración de riesgos, a fin de presentar los resultados de la evaluación ante la línea estratégica (Comité Institucional de Coordinación de Control Interno).


- IV. Revisión o revaloración del riesgo. Anualmente como resultado de los monitoreos trimestrales, el líder de proceso deberá evaluar la pertinencia de los riesgos identificados y de las actividades de control formuladas, y definir las actualizaciones requeridas. Esta actividad se deberá realizar máximo hasta el tercer mes de cada vigencia.

Adicionalmente, el líder y su equipo deberán revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados, para así proceder con la actualización del mapa de riesgos de su proceso.

El mapa de riesgos de corrupción se podrá ajustar durante el año de su vigencia cada vez que se identifique la necesidad, y su actualización se realizará anualmente con la formulación del Programa de transparencia y ética pública.

## 5.6 Tratamiento de riesgos materializados

En el evento de materialización de un riesgo, las líneas deberán emprender acciones en el marco de sus responsabilidades, así:

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 13 de 28

- Primera línea:

1. Informar a la segunda línea sobre la materialización detectada mediante el formato de monitoreo trimestral, remitiendo el respectivo plan de restablecimiento que incluya la ejecución de la corrección que permitió restablecer la situación y las acciones a adelantar para la actualización del mapa de riesgos.
2. Implementar el plan de restablecimiento definido, el cual podrá incluir la activación de los planes de recuperación del servicio definidos en el Plan de Continuidad de Negocio cuando el evento haya causado interrupción de actividades priorizadas para la entidad.
3. Cuando se trate de un riesgo de corrupción, realizar la denuncia ante la instancia de control correspondiente, una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normativa asociada al hecho de corrupción materializado).
4. Para los riesgos materializados relacionados con LA/FT/FP se realizará el Reporte de Operación Sospechosa – ROS, en la opción que corresponda (inicial, adición o corrección), y la respectiva denuncia ante la autoridad competente.


Nota: Los Reportes de Operación Sospechosa generados con ocasión a la gestión del Riesgo LA/FT/FP gozan de confidencialidad y únicamente serán compartidos al “Responsable de Cumplimiento” y el “Equipo de Cumplimiento y Debida Diligencia” por el canal habilitado haciendo uso de los formatos establecidos en las directrices de debida diligencia vigentes, los cuales posteriormente entrarán en flujo de reporte mediante la herramienta SIREL de la Unidad de Información y Análisis Financiero – UIAF.

- Segunda línea:

1. Consolidar y comunicar a la tercera línea sobre las materializaciones informadas por los líderes de proceso.
2. Verificar el cumplimiento de los planes de restablecimiento definidos.
3. Orientar a los líderes de proceso en la actualización del mapa de riesgos.
4. En articulación con la tercera línea, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados.

- Tercera línea:

1. Cuando en el marco de un ejercicio de evaluación independiente o seguimiento, la Oficina de Control Interno identifique la materialización de un riesgo, deberá informar a los líderes de proceso sobre el hecho detectado, los cuales emprenderán las acciones descritas para la primera línea en este numeral.
2. Informar a la segunda línea con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso para revisar el mapa de riesgos.
3. En articulación con la segunda línea, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 14 de 28

## 6. Responsabilidades y competencias

Conforme a lo definido por la dimensión de Control Interno del Modelo Integrado de Planeación y Gestión – MIPG, los roles y responsabilidades para la administración de riesgos están dados por el modelo de líneas, así<sup>10</sup>:

### ➤ Línea estratégica

Esta línea, al ser una instancia decisoria dentro del sistema de Control Interno, está bajo la responsabilidad de la alta dirección y del Comité Institucional de Coordinación de Control Interno; su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad. Por su parte, el Comité Institucional de Gestión y Desempeño analiza la gestión del riesgo y aplica las mejoras.

### ➤ Primera línea

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.

Le corresponde asegurarse de implementar la metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.


### ➤ Segunda línea

Soporta y guía la línea estratégica y la primera línea en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo una revisión independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de la revisión y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.).

Corresponde al área encargada de la gestión del riesgo (segunda línea) la difusión y asesoría de la presente metodología, así como la verificación del cumplimiento de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

El equipo SARLAFT, de la Subsecretaría de Gestión Institucional, acompañará metodológicamente la identificación de los riesgos de esta tipología, y a su vez complementará el desarrollo de las actividades requeridas en cumplimiento de las directrices vigentes en la materia que se definan para la prevención del riesgo de LA/FT/FP.

<sup>10</sup> "Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6. Departamento Administrativo de la Función Pública. Año 2022.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 15 de 28

➤ Tercera línea

Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea, cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. La tercera línea está conformada por la Oficina de Control Interno o auditoría interna.

Corresponde a las unidades de control interno, realizar evaluación independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos y los resultados de la evaluación de la gestión del riesgo.


La Oficina de Control Interno acompañará técnica y metodológicamente el desarrollo de las acciones derivadas de la gestión del riesgo.

7. Evaluación del lineamiento

La evaluación de la política de administración de riesgos se realiza anualmente y en dos niveles:

➤ Evaluación estratégica de la política de administración de riesgos:

Objetivos específicos de la Política	Método (indicador)	Responsable de la medición
Definir los criterios para identificar y gestionar los riesgos asociados a los procesos de la entidad.	<p>Nombre del indicador: <i>Eficacia en la gestión de riesgos de los procesos</i></p> <p>Fórmula:</p> $\frac{N^{\circ} \text{ de procesos con mapa de riesgos aprobado y vigente } *}{N^{\circ} \text{ de procesos institucionales}} \times 100$ <p>*Adoptado mediante acto administrativo y que no supere un año desde la fecha de aprobación.</p>	Subdirección de Diseño, Evaluación y Sistematización
Definir los criterios para establecer actividades de control preventivas, detectivas y correctivas para los riesgos identificados, con el fin de mitigar los posibles efectos de su materialización en el cumplimiento de las	<p>Nombre del indicador: <i>Eficacia en la formulación de actividades de control</i></p> <p>Fórmula:</p>	Subdirección de Diseño, Evaluación y Sistematización

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 16 de 28


Objetivos específicos de la Política	Método (indicador)	Responsable de la medición
disposiciones legales, la misión institucional y los objetivos estratégicos.	$\frac{N^{\circ} \text{ de mapas de riesgos con actividades de control vigentes}^{**}}{N^{\circ} \text{ de mapas de riesgos de los procesos}} \times 100$ <p>**Actividades de control en ejecución dentro del periodo establecido en el mapa (1 año)</p>	
Definir los criterios para actuar de manera oportuna ante la materialización de los riesgos identificados.	<p>Nombre del indicador: <i>Eficacia en el tratamiento de riesgos materializados</i></p> $\frac{N^{\circ} \text{ de planes de restablecimiento de riesgos ejecutados}}{N^{\circ} \text{ total de riesgos materializados detectados}^{***}} \times 100$ <p>*** Fuente de datos: formato de monitoreo trimestral.</p> <p>Nombre del indicador: <i>Efectividad de la gestión del riesgo</i></p> <p>Fórmula:  <math display="block">\frac{(N^{\circ} \text{ total de riesgos identificados} - N^{\circ} \text{ de riesgos materializados})}{N^{\circ} \text{ total de riesgos identificados}} \times 100</math> </p>	Subdirección de Diseño, Evaluación y Sistematización

➤ Evaluación táctica de la política de administración de riesgos:

Elemento a evaluar de la política	Método	Responsable
Implementación de la política	Medición del nivel de implementación del procedimiento Administración de Riesgos, código PCD-SG-003 (autoevaluación del procedimiento)	Líder del proceso Sistema de Gestión.

8. Administración del lineamiento


Subdirección de Diseño, Evaluación y Sistematización – Subdirección de Investigación e Información.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <hr/> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 17 de 28

## 9. Aprobación del documento

	Elaboró	Revisó	Aprobó
Nombre	<p>Viviana Lucía Mendoza Hortúa</p> <p>Juan Alberto Giraldo</p> <p>Pablo Leonardo Molano Parra</p>	<p>Elizabeth Soler Yaya</p> <p>Andrea Eliana Salazar Pérez</p> <p>Marcela Acosta Orjuela</p> <p>Lina María Sánchez Romero</p> <p>Andrés Penagos Guarnizo*</p> <p>Rosemary Chávez Rodríguez*</p>	<p>Comité Institucional de Coordinación de Control Interno</p>
Tipo de vinculación y cargo/rol	<p>Contratista Subdirección de Diseño, Evaluación y Sistematización – Gestora Proceso Sistema de Gestión</p> <p>Contratista Subdirección de Investigación e Información – Equipo seguridad de la información</p> <p>Contratista Subsecretaría de Gestión Institucional – Equipo SARLAFT</p>	<p>Subdirectora de Diseño, Evaluación y Sistematización – Líder Proceso Sistema de Gestión</p> <p>Subdirectora de Investigación e Información</p> <p>Contratista Subsecretaría de Gestión Institucional – Equipo SARLAFT</p> <p>Subsecretaria de Gestión Institucional</p> <p>Contratista Oficina de Control Interno Jefe Oficina de Control Interno *En rol de enfoque hacia la prevención y de evaluación a la gestión de riesgos.</p>	

\*Acta N° 01 - 20/06/2025 sesión ordinaria del Comité Institucional de Coordinación de Control Interno.


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 18 de 28

## ANEXOS

### Anexo 1. Recursos para riesgos de corrupción

Tabla 1: Hechos constitutivos de corrupción y sus riesgos asociados en la función administrativa del Estado

Descripción del hecho de corrupción	Riesgo de corrupción
Prometer, ofrecer o conceder directamente o por interpuesta persona a directivos, administradores, empleados o asesores de una sociedad, asociación o fundación, una dádiva o cualquier beneficio no justificado para que le favorezca a él o a un tercero.	Posibilidad de pérdida de gobernanza institucional y de la confianza pública en el Estado.
Proferir una resolución, dictamen o concepto manifiestamente contrario a la ley para favorecer intereses particulares.	Posibilidad de reducción de la capacidad de acción del Estado y de los organismos de administración de justicia, fomentando el delito.
Apropiarse en provecho suyo o de un tercero de bienes del Estado o de empresas o instituciones en que éste tenga parte o de bienes o fondos parafiscales, o de bienes de particulares cuya administración, tenencia o custodia se le haya confiado por razón o con ocasión de sus funciones.	Posibilidad de detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.
Intervención en el trámite, aprobación o celebración de un contrato con violación al régimen legal o a lo dispuesto en normas constitucionales, sobre inhabilidades o incompatibilidades.	Posibilidad de pérdida de confianza de la comunidad hacia las actuaciones públicas, limitando la capacidad de gestión del Estado.
Tramitar un contrato sin observancia de los requisitos legales esenciales o lo celebración o liquidación sin verificar el cumplimiento de los mismos.	Posibilidad de pérdida de confianza de la comunidad hacia las actuaciones públicas, limitando la capacidad de gestión del Estado.
Utilizar indebidamente, en provecho propio o de un tercero, influencias derivadas del ejercicio del cargo o de la función, con el fin de obtener cualquier beneficio de parte del servidor público en asunto que éste se encuentre conociendo o haya de conocer.	Posibilidad de pérdida de confianza de la comunidad hacia las actuaciones públicas, limitando la capacidad de gestión del Estado.
Reporte erróneo de información financiera con dolo o intención	Posibilidad de detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.
Incumplimiento premeditado de condiciones contractuales para conseguir beneficios extralegales.	Posibilidad de detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.
Actuaciones administrativas sin el lleno de los requisitos y sin evidencias trazables hechas con intención.	Posibilidad de investigaciones administrativas, disciplinarias y penales.
Pagos intencionales que no corresponden con el servicio recibido.	Posibilidad de detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 19 de 28


Descripción del hecho de corrupción	Riesgo de corrupción
Inobservancia de leyes, normas y/o lineamientos con la intención de obtener beneficios particulares.	Posibilidad de Pérdida de confianza de la comunidad hacia las actuaciones públicas, limitando la capacidad de gestión del Estado.
Inadecuada implementación del Sistema de Control Interno con la intención del obtener ventajas o beneficios ilegales.	Posibilidad de Pérdida de confianza de la comunidad hacia las actuaciones públicas, limitando la capacidad de gestión del Estado.
Cohecho	Posibilidad de Pérdida de confianza de la comunidad hacia las actuaciones públicas, limitando la capacidad de gestión del Estado.
Concusión	Posibilidad de Detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.
Facilitación del lavado de activos	Posibilidad de Reducción de la capacidad de acción del Estado y de los organismos de administración de justicia, fomentando el delito.
Facilitación del financiamiento a grupos terroristas o de operación ilegal	Posibilidad de Generación de obstáculos al desarrollo.
Celebración de transacciones extra-judiciales con reconocimiento de daños y perjuicios al contratista con cláusulas arbitrales en beneficio ilegal de un particular.	Posibilidad de Detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.
Testaferrato con beneficio para un servidor público de manera personal.	Posibilidad de Detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.
Testaferrato con beneficio para un particular con el consentimiento de un servidor público.	Posibilidad de Reducción de la capacidad de acción del Estado y de los organismos de administración de justicia, fomentando el delito.
Diseño de pliegos o estudios previos con un beneficio sesgado ilegalmente para favorecer a un tercero.	Posibilidad de Detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.
Suscripción de modificaciones (adiciones, adendas, otrosíes) que beneficien ilegalmente a un tercero.	Posibilidad de Detrimento patrimonial del Estado y pérdida de la capacidad de inversión en beneficio de la comunidad.
Uso de recursos públicos para la financiación de campañas políticas	Posibilidad de Pérdida de confianza de la comunidad hacia las actuaciones públicas, limitando la capacidad de gestión del Estado.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020. Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, anexo 4. DAFP.


## Anexo 2. Recursos para riesgos fiscales

Tabla 2: Puntos de riesgo fiscal y circunstancias inmediatas


<b>Puntos de Riesgo Fiscal</b> <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	<b>Circunstancia Inmediata</b> <i>Situación por la que se presenta el riesgo</i>
Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
Cumplimiento de obligaciones	Pago de Intereses moratorios

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 20 de 28

<b>Puntos de Riesgo Fiscal</b> <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	<b>Circunstancia Inmediata</b> <i>Situación por la que se presenta el riesgo</i>
Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
Suscripción de contratos	Sobrecostos en precios contractuales
Suscripción de contratos	Pagos efectuados a causa de riesgos previsible que debieron ser asignados al contratista en la matriz de riesgos previsible y no se le asignaron
Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
Suscripción de contratos	No exigir garantía única de cumplimiento contractual
Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 21 de 28

<b>Puntos de Riesgo Fiscal</b> <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	<b>Circunstancia Inmediata</b> <i>Situación por la que se presenta el riesgo</i>
Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas a contratistas
Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 22 de 28


<b>Puntos de Riesgo Fiscal</b> <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	<b>Circunstancia Inmediata</b> <i>Situación por la que se presenta el riesgo</i>
Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2022. Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, anexo 6. DAFP.

### Anexo 3. Recursos para riesgos de lavado de activos/financiación del terrorismo

Tabla 3: Ejemplos de situaciones que activan señales de alerta

<b>Señales de alerta</b>	<b>Situaciones</b>
Los documentos entregados por la contraparte están desactualizados o son incongruentes	El contratista o funcionario se rehúsa a llenar los formularios requeridos o a proporcionar la información necesaria para completarlos o a realizar la operación una vez que se le solicita llenar los formularios.
	Transferencias electrónicas hacia o por un individuo en la que la información sobre el originador o la persona en cuyo nombre se realiza la operación no es suministrada con la transferencia electrónica, cuando se espera la inclusión de tal información.
Información financiera atípica en la declaración de bienes y renta	Los estados financieros presentados por el contratista o funcionario revelan una situación financiera que difiere de aquella correspondiente a negocios similares.
	Múltiples transacciones llevadas a cabo en el mismo día en la misma institución financiera en un aparente intento de utilizar diferentes ventanillas, sin que exista una justificación para ello.
El contratista o funcionario se niega a informar sobre el origen de sus recursos	El contratista o funcionario que realiza frecuentemente operaciones por grandes sumas de dinero (depósitos, retiros o compras de instrumentos monetarios, entre otros) y se niega o evita dar información sobre el origen y/o destino del dinero o estas operaciones no guardan relación con su actividad económica.
	Existencia de cuentas individuales o mancomunadas de contratista o funcionario con relación de parentesco, que transfieren dinero entre sí, en forma periódica o eventual, con la instrucción de invertirse, cancelarse o transferirse al exterior a nombre de aquel que no cuenta con un origen regular de fondos producto de un negocio o de ingresos laborales consistentes a dichos montos.
	Transferencias en las cuales el beneficiario dice desconocer el nombre del remitente, el origen, el monto y la finalidad del dinero.
Contratista o funcionario que cuentan con un alto grado de liquidez y	El contratista o funcionario que realiza frecuentemente operaciones por grandes sumas de dinero (depósitos, retiros o compras de instrumentos monetarios, entre otros) y se niega o evita dar información sobre el origen y/o destino del dinero o estas operaciones no guardan relación con su actividad económica.

 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> SECRETARÍA DE INTEGRACIÓN SOCIAL	<b>PROCESO SISTEMA DE GESTIÓN</b>  <b>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</b>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 23 de 28


Señales de alerta	Situaciones
su actividad, de acuerdo con evaluación del mercado, normalmente no lo mantiene o genera.	Retiros por un monto significativo de una cuenta que había tenido poco movimiento o de una cuenta que recibió un depósito inusual.
	Cuentas que reciben depósitos periódicos y permanecen inactivas en otros periodos.
Realizan grandes inversiones, no obstante, haber sido creadas muy recientemente.	Compra o venta de diferentes bienes del activo fijo, dentro de un período corto, no concordante con el perfil del contratista o funcionario o sus actividades.
Personas jurídicas que presentan ingresos no operacionales superiores a los ingresos operacionales.	Una cuenta abierta por una persona jurídica o una organización que tiene la misma dirección de otras personas jurídicas u organizaciones, pero para la cual la misma persona o personas tienen firma autorizada, cuando no existe ninguna razón económica o legal aparente para tal tipo de acuerdo (por ejemplo, personas que fungen como directores para múltiples empresas cuyas sedes radican en el mismo lugar, entre otros supuestos.)
	Una cuenta abierta a nombre de una persona jurídica recientemente creada y en la cual se hacen depósitos más altos de los esperados en comparación con los ingresos de sus socios fundadores.
	Pólizas cuyo tomador o contratante son personas jurídicas o entidades que tienen la misma dirección, y para las cuales las mismas personas tienen firma autorizada a pesar de que no existe aparentemente ninguna razón económica o legal para ello.
Incremento exagerado en el volumen de ventas o ingresos sin una justificación aparente, después de atravesar por dificultades financieras	Compra o venta de diferentes bienes del activo fijo, dentro de un período breve, no concordante con el perfil del cliente o sus actividades.
	Depósito en efectivo con inmediata compra de cheques de viaje, órdenes de pago u otros instrumentos para el pago a terceros.
	Envíos de dinero frecuentes o en cantidades importantes, que no se pueden justificar fehacientemente, o que se realizan hacia o desde países comúnmente asociados con la producción, elaboración y venta de drogas, organizaciones terroristas o paraísos fiscales

Fuente: Documento Técnico: Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital, anexo 3. Secretaría General de la Alcaldía Mayor de Bogotá. 2022.

#### Anexo 4. Recursos para riesgos de seguridad de la información

Tabla 4: Amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Incidente importante	A, D, E
	Dstrucción de equipamiento o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climático Inundación	E
	Fenómenos sísmicos	E


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 24 de 28

Tipo	Amenaza	Origen
	Fenómeno volcánico	E
	Fenómeno meteorológico	E
Perdidas de los servicios esenciales	Falla de aire acondicionado o sistema de suministro de agua	A,D
	Pérdida de suministro de energía	A,D,E
	Falla de equipamiento de telecomunicaciones	A,D,E
Perturbación debida a la radiación	Radiación electromagnética	A,D,E
	Radiación térmica	D
	Pulsos electromagnéticos	D
Compromiso de la información	Interceptación de señales de interferencias comprometidas	D
	Espionaje remoto	D
	Escucha secreta	D
	Robo de medios o documentos	D
	Robo de equipos	D
	Recuperación de medios reciclados o descartados	D
	Divulgación	A,D
	Datos de fuentes poco fiables	A,D
	Manipulación ( <i>tampering</i> ) con hardware	D
	Manipulación ( <i>tampering</i> ) con software	A,D
Detección de posición	D	
Fallas técnicas	Fallas de equipo	A
	Mal funcionamiento del equipo	A
	Saturación de sistema de información	A,D
	Mal funcionamiento de software	A
	Brecha/fisura de mantenimiento de sistema de información	A,D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta de software	D
	Uso de software falsificado o copiado	A,D
	Corrupción de datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A,D
	Falsificación de derechos	D
	Negación de acciones	D
	Brecha de disponibilidad de personal	A,D,E

Fuente: ISO/IEC 27005:2018

Tabla 5. Amenazas dirigidas por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Desafío Ego Rebelión Estatus Dinero	- Hacking - Ingeniería social - Intrusión de Sistema, irrupciones - Acceso no autorizado a sistema
Delito informático	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de datos	- Delito informático (por ejemplo, acoso cibernético) - Acto fraudulento (por ejemplo, repetición, personificación, interceptación) - Soborno de información - Engaño - Intrusión de sistemas

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 25 de 28


Fuente de amenaza	Motivación	Acciones amenazantes
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cobertura mediática	Bomba/Terrorismo - Guerra de información - Ataque de sistema (por ejemplo, negación distribuida de servicio) - Penetración de sistema - Manipulación ( <i>tampering</i> ) de sistema
Espionaje industrial (Inteligencia, compañías, gobiernos extranjeros, otros intereses del gobierno)	Ventaja competitiva Espionaje económico	- Ventaja de Defensa - Ventaja Política - Explotación económica - Robo de información - Intrusión en privacidad personal - Ingeniería social - Penetración de sistema - Acceso no autorizado al sistema (acceso a información clasificada, propietaria, y/o relacionada con tecnología)
Internos (empleados pobremente entrenados, descontentos, maliciosos, negligentes, deshonestos, o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (Por ejemplo, error de entrada de datos, error de programación)	- Asalto a un empleado - Chantaje - Mirada a información propietaria - Abuso de computadora - Fraude y robo - Soborno de información - Entrada de datos falsificados, corruptos - Interceptación - Código malicioso (Por ejemplo, virus, bomba lógica, caballo de Troya) - Venta de información personal - Errores de sistema - Intrusión de sistema - Sabotaje de sistema - Acceso no autorizado a sistema

Fuente ISO/IEC 27005:2018


Tabla 6. Vulnerabilidades

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de esquemas periódicos de reemplazo	Destrucción de equipo o medios
	Susceptibilidad a humedad, Polvo, corrosión,	Polvo, suciedad, congelamiento
	Sensibilidad a radiación electromagnética	Radiación electromagnética
	Falta de control eficiente de cambio de configuración	Error en uso
	Susceptibilidad a variaciones de voltaje	Pérdida de suministro de voltaje
	Susceptibilidad a variaciones de temperatura	Fenómeno meteorológico
	Almacenamiento no protegido	Robo de medios o documentos
	Falta de cuidado en eliminación	Robo de medios o documentos
Copiado no controlado	Robo de medios o documentos	
Software	Falta o insuficiente prueba de software	Abuso de derechos
	Fallas bien conocidas en el software	Abuso de derechos
	No se cierra la sesión cuando se abandona la estación de trabajo	Abuso de derechos
	Eliminación o reutilización de medios de almacenamiento sin borrado apropiado	Abuso de derechos
	Falta de seguimiento de auditoría	Abuso de derechos
	Incorrecta asignación de derechos de acceso	Abuso de derechos
	Software ampliamente distribuido	Corrupción de Datos
Aplicación de programas de aplicación a datos erróneos en términos de tiempo	Corrupción de Datos	


Clasificación: Información Pública

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 26 de 28

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Complicada interface de usuario	Error en uso
	Falta de documentación	Error en uso
	Establecer parámetros incorrectos	Error en uso
	Fechas incorrectas	Error en uso
	Falta de mecanismos de identificación y autenticación como autenticación de usuario	Falsificación de derechos
	Tablas de contraseñas no protegidas	Falsificación de derechos
	Manejo / pobre de contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento de Software
	Habilitación de servicios innecesarios Procesamiento ilegal de datos Software nuevo o inmaduro	Mal funcionamiento de Software
	Especificaciones poco claras o incompletas para desarrolladores	Mal funcionamiento de Software
	Falta de control de cambio efectivo	Mal funcionamiento de Software
	Descarga y uso no controlado de software	Manipulación ( <i>tampering</i> ) con software
	Falta de copias de respaldo	Manipulación ( <i>tampering</i> ) con software
Falta de protección física del edificio, puertas y ventanas	Robo de medios o documentos	
Falla en producir reportes de gestión	Uso no autorizado de equipos	
Red	Falta de prueba de envío o recepción de un mensaje	Negación de acción
	Líneas de comunicación desprotegidas	Escucha ( <i>Eavesdropping</i> )
	Tráfico sensible desprotegido	Escucha ( <i>Eavesdropping</i> )
	Pobre conjunto de cableado	Falla en el equipo de telecomunicaciones
	Punto único de falla	Falla en el equipo de telecomunicaciones
	Falta de identificación y autenticación del remitente y el receptor	Falsificación de derechos
	Inseguridad en la arquitectura de la red	Espionaje remoto
	Transferencia de contraseñas en claro Espionaje	Espionaje remoto
	Inadecuada gestión de red (Resiliencia de ruteo)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado de equipos
Personal	Ausencia de personal	Brecha de disponibilidad de personal
	Procedimientos inadecuados de reclutamiento	Destrucción de equipamiento o medios
	Entrenamiento insuficiente en seguridad	Error en uso
	Uso incorrecto de software y hardware	Error en uso
	Falta de conciencia de seguridad	Error en uso
	Falta de mecanismos de seguimiento	Procesamiento ilegal de datos
	Trabajo no supervisado por personal externo o de limpieza	Robo de medios o documentos

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C.</p> <p>SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN</p> <p>LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 27 de 28

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	Uso no autorizado de equipamiento
Local	Uso inadecuado o descuidado de control de acceso físico a edificios y recintos	Dstrucción de equipamiento o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red de energía inestable	Pérdida de suministro de energía
	Falta de protección física del edificio, puertas y ventanas	Robo de equipamiento
	Falta de procedimiento formal para registro de usuarios y su baja	Abuso de derecho
	Falta de proceso formal para revisión de derechos de acceso (supervisión)	Abuso de derechos
	Falta o insuficientes capítulos (concernientes a seguridad) en contratos con clientes y/o terceros	Abuso de derechos
	Falta de procedimiento de seguimiento de instalaciones de procesamiento de la información	Abuso de derechos
Organización	Falta de auditorías regulares (supervisión)	Abuso de derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de derechos
	Falta de reportes de fallas registrados en bitácoras del administrador y operador	Abuso de derechos
	Respuesta inadecuada de mantenimiento de servicio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta o insuficiente Acuerdo de Nivel de Servicio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de procedimiento de control de cambio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de procedimiento formal para control de la documentación del SGSI	Corrupción de datos
	Falta de procedimiento formal para la supervisión de los registros del SGSI	Corrupción de datos
	Falta de proceso formal para autorización de información públicamente disponible	Datos de fuentes no confiables
	Falta de asignación apropiada de responsabilidades por la seguridad de la información	Negación de acciones
	Falta de planes de continuidad	Falla de equipamiento
	Falta de política de uso de e-mail	Error en uso
	Falta de procedimientos para introducir software a sistemas operacionales	Error en uso
Falta de registros en bitácoras del administrador y operador	Error en uso	

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO SISTEMA DE GESTIÓN LINEAMIENTO ADMINISTRACIÓN DE RIESGOS</p>	Código: LIN-SG-001
		Versión: 4
		Fecha: Memo I2025020984 – 26/06/2025
		Página: 28 de 28

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Falta de procedimientos para manejo de información clasificada	Error en uso
	Falta de responsabilidades de seguridad de la información en descripciones de puestos	Error en uso
	Falta o insuficientes estipulaciones (concernientes a seguridad de la información) en contratos con empleados	Procesamiento de datos ilegal
	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Robo de equipamiento
	Falta de política formal sobre uso de computadoras móviles	Robo de equipamiento
	Falta de control de activos fuera de las instalaciones	Robo de equipamiento
	Falta o insuficiente política de escritorio y pantalla limpia	Robo de medios o documentos
	Falta de autorización a las instalaciones de procesamiento de la información	Robo de medios o documentos
	Falta de mecanismos de seguimiento establecidos para brechas de seguridad	Robo de medios o documentos
	Falta de revisiones regulares de gestión	Uso no autorizado de equipamiento
	Falta de procedimientos para reportar debilidades de la seguridad	Uso no autorizado de equipamiento
	Falta de procedimientos de estipulación de cumplimiento con derechos de propiedad intelectual	Uso de software falso o copiado

Fuente: ISO/IEC 27005:2018