

**MEMORANDO**

(150)

Bogotá D.C., mayo 29 de 2026

**PARA:** Dr. GUSTAVO QUINTERO ARDILA  
Secretario Distrital de Gobierno

**DE:** JEFE OFICINA DE CONTROL INTERNO

**ASUNTO:** Informe de Seguimiento Informe de Seguimiento a la Gestión del Riesgo

Respetado doctor.

De manera atenta, en cumplimiento con lo establecido en el Plan Anual de Auditoría Interna – PAAI 2026, atentamente me permito remitir informe de seguimiento a la gestión del riesgo, con el fin de que sea socializado con su equipo de trabajo analizando su contenido y se tomen las respectivas acciones de mejora que a su consideración apliquen para el proceso evaluado.

Este informe se da a conocer al señor Secretario en cumplimiento de lo dispuesto en el Decreto 338 de 2019 *“Por el cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción ARTÍCULO 1. PARÁGRAFO 1. Los informes de auditoría, seguimientos y evaluaciones tendrán como destinatario principal el representante legal de la entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva, y deberán ser remitidos al nominador cuando este lo requiera”*.

Finalmente, se informa que, el presente informe fue comunicado a la Oficina Asesora de Planeación mediante la Radicado No. 20261500202923 y a la Dirección de Tecnología e Información mediante la comunicación No. 20261500203213. En cumplimiento de los principios de transparencia y publicidad, el informe se encuentra publicado en la página web institucional. <https://www.gobiernobogota.gov.co/transparencia/planeacion-presupuesto-informes/informes-oficina-control-interno/otros-informes-consultas-a-bases-de-datos-o-sistemas-de-informacion/informes-de-ley-o-seguimiento>.

Agradecemos su gestión, con el objetivo de fortalecer el Sistema de Control Interno de la Entidad.

Cordialmente,

(ORIGINAL FIRMADO)

**LADY JOHANNA MEDINA MURILLO**

Jefe Oficina de Control Interno

Anexo: Informe de seguimiento a la gestión del riesgo.

Elaboró: Deissy Liliana Sotelo- Contratista OCI

Yeina Rocío Aviles Barreiro – Contratista OCI

Revisó/aprobó: Lady Johanna Medina Murillo – Jefe OCI

**INFORME DE SEGUIMIENTO A LA GESTIÓN DEL RIESGO****Destinatarios**

- Gustavo Alberto Quintero Ardila - Secretario Distrital De Gobierno
- Diego Fernando Figueroa – Jefe Oficina Asesora de Planeación
- Mario Alexander Ortiz Salgado – Director de Tecnologías e Información

**1. Objetivos****1.1. Objetivo General**

Realizar evaluación a la aplicabilidad de la Política de Administración del Riesgo de la Secretaría Distrital de Gobierno, incluyendo los riesgos de corrupción y seguridad de la Información con el fin de verificar su identificación, análisis, valoración, tratamiento y monitoreo, conforme a los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas y demás disposiciones aplicables.

**1.2. Objetivos Específicos**

- Realizar verificación y análisis de la información aportada por la Oficina Asesora de Planeación y la Dirección de Tecnología e Información, producto de la ejecución de las diferentes etapas de la gestión del riesgo.
- Emitir observaciones y/o recomendaciones con relación a los resultados obtenidos en el seguimiento de la gestión del riesgo en la entidad.

**2. Alcance**

El presente seguimiento comprende la verificación de la implementación de la Política de Administración del Riesgo en los procesos de la Secretaría Distrital de Gobierno, mediante la revisión de los mapas de riesgos de gestión, corrupción y seguridad de la Información correspondientes a la vigencia 2025.

La evaluación se centrará en la identificación, análisis, valoración, definición de controles y acciones de tratamiento, así como en los mecanismos de monitoreo y seguimiento definidos por los líderes de proceso.

El ejercicio se realizará con base en la información documentada y registrada en las matrices institucionales de riesgos y en los soportes reportados por las dependencias responsables durante la vigencia evaluada.

**3. Marco normativo o criterios del informe**

Ley 87 de 1993

Ley 1474 de 2011

Decreto 648 de 2017

Decreto 1122 de 2024

"Guía para la Gestión Integral del Riesgo en Entidades Públicas / Versión 07 - 2025"

#### 4. Equipo auditor:

Deissy Liliana Sotelo Torres - OCI  
Yeina Rocio Aviles Barreiro – OCI

#### 5. Metodología

- Se emitió aviso de inicio de seguimiento y la solicitud de información mediante memorando dirigido a la Oficina Asesora de Planeación, y a través de correo electrónico remitido a la Dirección de Tecnología de la Información. La información requerida correspondía a la documentación y a los mapas de riesgos de la Entidad en el Nivel Central y Nivel Local.
- Una vez las dependencias remitieron la documentación a través de las carpetas compartidas en OneDrive habilitadas por la Oficina de Control Interno, se procedió con el análisis documental y la consulta de los mapas de riesgos. En este proceso se evaluaron las diferentes etapas relacionadas con la identificación y valoración de riesgos, la efectividad de los controles y monitoreos realizados durante la vigencia 2025, así como el cumplimiento de los requisitos normativos y de los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 07 – 2025.
- Finalizado el análisis de la información y el muestreo de evidencias, se registraron los resultados, observaciones y recomendaciones en el informe de seguimiento.

#### 6. Periodo de ejecución

Entre el 01 de marzo hasta el 30 de mayo 2026.

#### 7. Desarrollo

La Oficina de Control Interno, en cumplimiento de sus funciones de evaluación y seguimiento, presenta los resultados de la verificación del avance y la efectividad de la gestión integral del riesgo implementada por la entidad. Este seguimiento permite identificar oportunidades de mejora, así como evaluar el grado de cumplimiento de las acciones definidas por la administración para la mitigación de los riesgos identificados, contribuyendo al fortalecimiento del Sistema de Control Interno y al logro de los objetivos institucionales.

El presente seguimiento contiene los resultados de la revisión de la Política Integral de Gestión del Riesgo de la Entidad, así como de la identificación y clasificación de los riesgos en sus diferentes tipologías: riesgos generales de gestión, riesgos de seguridad de la información y riesgos fiscales.

Asimismo, se presentan los resultados relacionados con la identificación y evaluación de los riesgos, la descripción y efectividad de los controles, y los resultados de los monitoreos realizados, de conformidad con los requisitos normativos aplicables y los lineamientos establecidos en la *Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 07 – 2025*, emitida por el DAFP.

### 7.1. Resultados de la revisión de la Política de Administración del Riesgo

En cumplimiento de los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo, se realizó un análisis comparativo entre los requisitos mínimos definidos para la formulación de la Política y lo contenido en el documento interno PLE-PIN-M001 V9 Manual de Gestión del Riesgo.

El análisis permitió evidenciar que el documento evaluado incorpora varios elementos metodológicos asociados a la administración del riesgo, particularmente en aspectos relacionados con la identificación, valoración, tratamiento y seguimiento de riesgos institucionales. No obstante, frente al enfoque fortalecido que incorpora la Guía V7, basado en los principios de gobernanza, cultura organizacional del riesgo, se identifican oportunidades de fortalecimiento frente al enfoque de gestión integral del riesgo definido en la Guía V7, particularmente en componentes asociados a gobernanza, cultura del riesgo, madurez institucional, articulación con MIPG y aplicación del enfoque COSO-ERM., entre los principales aspectos a fortalecer se encuentran:

- La articulación integral con el Modelo Integrado de Planeación y Gestión – MIPG
- El desarrollo del análisis de contexto interno y externo
- La incorporación de estrategias de cultura y apropiación del riesgo
- La definición de mecanismos formales de comunicación y reporte
- La implementación de indicadores clave de riesgo (KRI)
- El fortalecimiento del enfoque de mejora continua.

De igual manera, aunque el documento desarrolla elementos asociados a riesgos de corrupción y soborno, la Guía V7 amplía el alcance hacia una gestión integral del riesgo, incluyendo riesgos de integridad pública, riesgos fiscales, riesgos de seguridad de la información y demás tipologías estratégicas que deben gestionarse de manera articulada.

En términos generales, se concluye que el documento PLE-PIN-M001 V9 presenta avances en la implementación metodológica de la gestión integral del riesgo; no obstante, se evidencian oportunidades de fortalecimiento en componentes estratégicos, operativos y de gobernanza definidos en la Guía V7, evidenciándose una estructura metodológica funcional, pero con necesidad de fortalecimiento y armonización en componentes estratégicos, de gobernanza y de madurez institucional para lograr una alineación integral con el enfoque actualizado definido por Función Pública. A continuación, se presentan los resultados de la revisión frente al cumplimiento de los criterios definidos en la Guía para la Gestión Integral del Riesgo V7 – 2025.

Tabla 1. Verificación estructura de la política de gestión del riesgo

1. POLÍTICA DE GESTIÓN DEL RIESGO		
Requisito Guía Riesgos V7	Cumplimiento en PLE-PIN-M001 V9	Observación OCI
Definir objetivo del sistema de riesgos	Cumple	El manual define objetivo general y específicos
Definir alcance (procesos, actores, jurisdicción)	Cumple	Aplica a todos los procesos y niveles institucionales
Incluir enfoque de integridad pública	Parcial	El alcance definido aplica a los procesos del Nivel Central y Alcaldías Locales e incluye riesgos de gestión, corrupción, soborno, seguridad digital y ambiental; sin embargo, frente a los lineamientos de la Guía para la Gestión Integral del Riesgo V7, se recomienda desarrollar integralmente el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, el cual incorpora amenazas asociadas a corrupción, fraude, conflicto de interés, soborno y LA/FT/FP. Así mismo, no

		<p>define de manera clara actores, líneas de defensa, responsabilidades estratégicas ni su articulación con MIPG y los mecanismos de monitoreo, seguimiento y mejora continua.</p> <p>Considerando que actualmente se encuentra vigente la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025), la OCI recomienda que, en las futuras actualizaciones del Manual de Gestión del Riesgo, se incorporen los lineamientos, enfoques y requisitos establecidos en esta versión, de conformidad con los plazos y disposiciones definidos por la entidad para su adopción.</p>
Definir marco de apetito del riesgo	Parcial	<p>El documento incorpora definiciones sobre capacidad, apetito y tolerancia del riesgo; sin embargo, frente a los lineamientos de la Guía para la Gestión Integral del Riesgo V7, su desarrollo es principalmente conceptual y no se evidencian mecanismos operativos para su implementación institucional.</p> <p>No se identifican niveles específicos de apetito y tolerancia por tipología de riesgo, límites para la toma de decisiones, herramientas de medición, mecanismos de monitoreo ni articulación con objetivos estratégicos y procesos institucionales. Así mismo, aunque se señala que la tolerancia del riesgo debe ser aprobada por la Alta Dirección, no se evidencian responsabilidades ni lineamientos operativos para su aplicación y seguimiento.</p> <p>En consecuencia, se concluye que el documento desarrolla el componente conceptual, pero no evidencia su implementación y monitoreo conforme a los requisitos establecidos en la Guía V7.</p>
<b>2. ROLES Y RESPONSABILIDADES (LÍNEAS DE DEFENSA)</b>		
<b>Requisito Guía Riesgos V7</b>	<b>Cumplimiento en PLE-PIN-M001 V9</b>	<b>Observación OCI</b>
Definir líneas de defensa (1ra, 2da, 3ra)	Parcial	<p>Si bien el documento desarrolla conceptualmente las líneas de defensa, no se evidenció, dentro de la muestra revisada, exista formalización suficiente de mecanismos de articulación, monitoreo independiente, trazabilidad, escalamiento y segregación funcional entre líneas de defensa conforme al enfoque definido en la Guía V7 y MECL.</p> <p>Así mismo, no se evidencian mecanismos sólidos de articulación, supervisión, escalamiento ni trazabilidad entre las líneas de defensa, particularmente en lo relacionado con seguimiento metodológico, monitoreo de controles y gestión de riesgos. En consecuencia, se concluye que el modelo se encuentra principalmente documentado, pero no implementado integralmente en la operación del sistema de gestión del riesgo.</p> <p>En virtud de lo anterior se evidencia insuficiencia en la formalización de protocolos de escalamiento y reporte entre la Primera y Segunda Línea, y entre la Segunda y Tercera Línea. Esto es una brecha de actualización normativa del manual (V9 → Guía V7).</p>
Definir responsables del sistema	Cumple	Incluye líderes de proceso, oficial de cumplimiento y control interno
Rol de auditoría interna	Cumple	Se contempla auditoría de riesgos
<b>3. CONTEXTO Y FACTORES DE RIESGO</b>		
<b>Requisito Guía Riesgos V7</b>	<b>Cumplimiento en PLE-PIN-M001 V9</b>	<b>Observación OCI</b>
Análisis de contexto interno y externo	Parcial	Aunque el documento menciona el análisis de contexto, no se evidenció desarrollo metodológico integral asociado a variables estratégicas, entorno regulatorio, factores internos y externos, partes interesadas y capacidades institucionales requeridas por la Guía V7.

Identificación de factores de riesgo (tabla estándar)	Cumple	Usa factores similares: procesos, talento humano, tecnología, etc.
Inclusión de riesgos de integridad pública	Parcial	De acuerdo con la revisión realizada a la documentación aportada, se evidenció que su contenido se encuentra alineado con los lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 (2022), la cual corresponde al marco metodológico vigente al momento de su implementación. No obstante, considerando que actualmente se encuentra vigente la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025), se recomienda que, en las futuras actualizaciones del Manual de Gestión del Riesgo, se incorporen los lineamientos, enfoques y requisitos establecidos en esta versión, de conformidad con los plazos y disposiciones definidos por la entidad para su adopción.
<b>4. IDENTIFICACIÓN DEL RIESGO</b>		
Requisito Guía Riesgos V7	Cumplimiento en PLE-PIN-M001 V9	Observación OCI
Identificación basada en procesos	Cumple	Asociado a procesos institucionales
Estructura estándar de redacción del riesgo	Cumple	Usa estructura “Posibilidad De...”
Inclusión de causas y consecuencias	Cumple	Se contemplan causas raíz y efectos
<b>5. ANÁLISIS Y VALORACIÓN DEL RIESGO</b>		
Requisito Guía Riesgos V7	Cumplimiento en PLE-PIN-M001 V9	Observación OCI
Evaluación de probabilidad e impacto	Cumple	Se utilizan escalas definidas
Determinación de riesgo inherente	Cumple	Incluido metodológicamente
Uso de matrices de riesgo	Cumple	Incluye mapa de calor y matrices
<b>6. CONTROLES</b>		
Requisito Guía Riesgos V7	Cumplimiento en PLE-PIN-M001 V9	Observación OCI
Identificación de controles (preventivos, detectivos, correctivos).	Parcial	Se identificaron eventos de riesgo materializados y recurrentes, lo que evidencia oportunidades de fortalecimiento en el diseño, formalización, ejecución, documentación o monitoreo de los controles implementados.
Evaluación de diseño y efectividad de controles	Parcial	No se evidencia evaluación detallada de atributos del control.
Relación control – causa raíz	Parcial	No se evidenció, de manera consistente, articulación metodológica entre controles definidos y causas raíz identificadas dentro de los mapas de riesgos.
<b>7. TRATAMIENTO DEL RIESGO</b>		
Requisito Guía Riesgos V7	Cumplimiento en PLE-PIN-M001 V9	Observación OCI
Definir opciones de tratamiento (evitar, reducir, compartir, aceptar)	Cumple	Especial énfasis en evitar/reducir soborno

Planes de tratamiento	Parcial	<p>El Manual de Gestión del Riesgo PLE-PIN-M001 V9 incorpora lineamientos generales sobre tratamiento del riesgo, incluyendo opciones de manejo como aceptar, evitar, compartir y reducir el riesgo, así como referencias al riesgo residual y responsabilidades de la primera línea de defensa. Sin embargo, no se evidenció cumplimiento frente a la generación de acciones derivadas de la materialización de riesgos.</p> <p>Aunque el documento desarrolla conceptualmente el tratamiento del riesgo, presenta debilidades frente a los lineamientos de la Guía para la Gestión Integral del Riesgo V7, debido a que no define criterios claros para priorización, seguimiento, monitoreo del riesgo residual, indicadores de efectividad ni tratamiento diferencial por tipología de riesgo.</p> <p>En consecuencia, se concluye que el documento presenta un cumplimiento parcial frente a los requisitos metodológicos, operativos y de seguimiento establecidos en la Guía V7.</p>
Evaluación costo-beneficio	Parcial	Se menciona, pero no se desarrolla ampliamente

#### 8. MONITOREO Y SEGUIMIENTO

Requisito Guía Riesgos V7	Cumplimiento en PLE-PIN-M001 V9	Observación OCI
Monitoreo periódico de riesgos	Parcial	Monitoreo cuatrimestral definido para riesgos de gestión y corrupción, no se encuentra definido para riesgos de seguridad de la información.
Revisión por líneas de defensa	Cumple	Primera, segunda y tercera línea
Mejora continua del sistema	Cumple	Implícita, se recomienda incorporar temas relacionados con SIGRIP

#### 9. SOPORTE (RECURSOS, DOCUMENTACIÓN, COMPETENCIAS)

Requisito Guía Riesgos V7	Cumplimiento en PLE-PIN-M001 V9	Observación OCI
Definición de recursos (humanos, tecnológicos)	Parcial	No está claramente estructurado como lo exige la guía
Competencias del personal	Parcial	No está detallado
Estrategia de comunicación y formación	Parcial	No se evidencia claramente un capítulo o sección específica a la estrategia de comunicación y consulta como proceso habilitador transversal, como lo menciona la Guía de Riesgos V7-2025

Fuente: Elaboración propia OCI con base en reporte de la OAP

## 7.2. Clasificación de riesgos por tipología.

En el seguimiento realizado por la Oficina de Control Interno, se efectuó la verificación de los documentos y mapas de riesgos correspondientes al Nivel Central y a las Alcaldías Locales, suministrados por la Oficina Asesora de Planeación y la Dirección de Tecnologías de la Información.

Como resultado del análisis, se evidenció que la Entidad cuenta con un total de 200 riesgos y 358 controles, distribuidos en 38 mapas de riesgos. Del total de riesgos identificados, el 51% corresponde a riesgos generales de gestión, el 34 % a riesgos de seguridad de la información y el 15 % restante a riesgos de corrupción, tal como se presenta a continuación:

Tabla 2. Clasificación riesgos de acuerdo con su tipología

CLASIFICACIÓN RIESGOS DE ACUERDO CON SU TIPOLOGÍA			
CLASIFICACIÓN	CANTIDAD DE RIESGOS IDENTIFICADOS	CANTIDAD DE CONTROLES IDENTIFICADOS	CANT. MAPAS DE RIESGOS
Riesgos de Gestión	102	137	19
Riesgos de corrupción	30	41	1
Riesgos Seguridad de la información	68	180	18
<b>TOTAL</b>	<b>200</b>	<b>358</b>	<b>38</b>

Fuente: Elaboración propia OCI con base en reporte de la OAP Y DTI

### Gestión Preventiva del Riesgo Fiscal

En cumplimiento de los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 y en concordancia con lo señalado en la Ley 610 de 2000 respecto al daño patrimonial al Estado, la Oficina de Control Interno realizó revisión de la incorporación de la gestión preventiva del riesgo fiscal dentro de la Política Integral de Gestión del Riesgo y de las matrices institucionales de riesgos de la Entidad.

Producto de la verificación efectuada, se evidenció que el documento PLE-PIN-M001 V9 incorpora de manera general la administración del riesgo institucional; no obstante, frente al enfoque específico de gestión preventiva del riesgo fiscal definido en la Guía V7, se identifican oportunidades de fortalecimiento relacionadas con la identificación, análisis y tratamiento diferencial de esta tipología de riesgo.

Durante la revisión documental no se evidenció metodología específica orientada a:

- La identificación de puntos de riesgo fiscal asociados a procesos con incidencia en la gestión fiscal.
- La definición de circunstancias inmediatas que puedan generar daño patrimonial al Estado.
- La articulación metodológica entre riesgos fiscales y procesos relacionados con ejecución presupuestal, contratación, supervisión contractual, gestión de bienes, pagos, almacén, inventarios y demás actividades con incidencia sobre recursos públicos.
- La incorporación de controles preventivos específicos orientados a mitigar riesgos de detrimento patrimonial.
- El establecimiento de mecanismos de monitoreo y seguimiento diferencial para riesgos fiscales.

Así mismo, aunque las matrices institucionales incluyen riesgos asociados a procesos administrativos y financieros, no se evidenció clasificación o tratamiento específico que permita identificar claramente los riesgos fiscales conforme a los lineamientos establecidos en el Capítulo IV de la Guía para la Gestión Integral del Riesgo V7.

De igual manera, no se observaron criterios metodológicos documentados para:

- Determinar el impacto patrimonial potencial.
- Identificar bienes, recursos o intereses económicos susceptibles de afectación.

- Priorizar riesgos fiscales de acuerdo con su severidad o exposición.
- Definir indicadores de seguimiento asociados a riesgos fiscales.

En consecuencia, se concluye que la Entidad presenta avances generales en materia de administración del riesgo; sin embargo, requiere fortalecer la incorporación del enfoque preventivo de riesgo fiscal mediante la adopción de herramientas metodológicas, controles y mecanismos de seguimiento alineados con los lineamientos definidos por Función Pública y el marco normativo aplicable.

#### - **Gestión del Riesgo en el Nivel Local**

En la verificación realizada por la Oficina de Control Interno se evidenció que el Nivel Local no cuenta con un enfoque diferencial claramente estructurado para la gestión del riesgo frente al Nivel Central, pese a las particularidades operativas, administrativas y territoriales propias de las Alcaldías Locales.

En relación con los riesgos de gestión, de los 19 mapas de riesgos existentes, cuatro tienen alcance en el nivel local, correspondientes a los procesos de Inspección, Vigilancia y Control; Gestión Corporativa Institucional; Gestión Pública Territorial Local; y Acompañamiento a la Gestión Local.

Por su parte, los riesgos de corrupción se encuentran consolidados en una única matriz institucional; no obstante, no se evidenció segregación metodológica o trazabilidad suficiente que permita identificar claramente aquellos riesgos asociados específicamente al Nivel Central y aquellos con incidencia directa en el Nivel Local.

En cuanto a los riesgos de seguridad de la información, la documentación aportada por la Dirección de Tecnologías de la Información evidencia la existencia de cinco mapas de riesgos asociados a las Alcaldías Locales de Barrios Unidos, San Cristóbal, Engativá, Puente Aranda y Teusaquillo, lo que evidencia una implementación parcial, gradual y no homogénea del componente de riesgos de seguridad de la información en las Alcaldías Locales.

En consecuencia, se considera necesario fortalecer el enfoque diferencial y territorial de la gestión del riesgo en el Nivel Local, promoviendo mecanismos que permitan a cada Alcaldía Local identificar, analizar, valorar, tratar y monitorear sus riesgos conforme a sus particularidades operativas, administrativas, territoriales y de prestación del servicio.

En este sentido, se recomienda:

- Promover la elaboración y actualización de matrices de riesgos específicas para cada Alcaldía Local, considerando su contexto territorial, operativo y administrativo.
- Fortalecer ejercicios de identificación y valoración de riesgos propios del Nivel Local, evitando la réplica automática de riesgos definidos para el Nivel Central sin análisis diferencial.
- Incrementar la participación de las Alcaldías Locales en las etapas de identificación, análisis, tratamiento, monitoreo y seguimiento de riesgos.
- Definir lineamientos metodológicos que permitan diferenciar claramente responsabilidades, riesgos, controles y mecanismos de monitoreo entre el Nivel Central y el Nivel Local.
- Fortalecer la articulación entre las líneas de defensa en el Nivel Local, garantizando mecanismos de seguimiento, trazabilidad y monitoreo de riesgos.

Lo anterior evidencia la necesidad de fortalecer el enfoque integral y territorial de la gestión del riesgo, en concordancia con los principios de gobernanza, prevención, articulación institucional y mejora continua establecidos en la Guía para la Gestión Integral del Riesgo V7.

### **7.2.1. Gestión Integral de Riesgos Generales de Gestión.**

#### **7.2.1.1. Herramientas para la Gestión del Riesgo**

En relación con la gestión de riesgos generales de gestión, la Entidad cuenta con instrumentos metodológicos y documentales orientados a la identificación, análisis, valoración, tratamiento y monitoreo de riesgos, soportados principalmente en los siguientes documentos institucionales:

- PLE-PIN-M001 Manual de Gestión del Riesgo.
- PLE-PIN-P015 Administración y Monitoreo de Riesgos de Gestión y Corrupción.
- PLE-PIN-F035 Formato Matriz Monitoreo de Riesgos.
- Diecinueve (19) mapas de riesgos de gestión asociados a los diferentes procesos institucionales.

Lo anterior evidencia la existencia de herramientas institucionales orientadas a soportar metodológicamente la gestión integral del riesgo en los procesos del Nivel Central y Nivel Local.

**Análisis de Contexto y DOFA:** De acuerdo con la revisión documental efectuada, se evidenció que los formatos PLE-PIN-F001 incorporan elementos relacionados con el análisis de contexto de los procesos, incluyendo aspectos internos y externos que pueden impactar el cumplimiento de los objetivos institucionales. Así mismo, se observaron ejercicios asociados al análisis DOFA como insumo para la identificación y valoración de riesgos, permitiendo reconocer debilidades, oportunidades, fortalezas y amenazas relacionadas con la operación de los procesos.

Lo anterior evidencia avances en la incorporación del análisis de contexto dentro de la gestión del riesgo, en concordancia con los lineamientos definidos en la Guía para la Gestión Integral del Riesgo V7, particularmente frente a la identificación de factores que pueden afectar el logro de objetivos institucionales, operativos y estratégicos.

No obstante, se identifican oportunidades de fortalecimiento relacionadas con la formalización metodológica del análisis de contexto, particularmente frente a:

- identificación de partes interesadas,
- análisis del entorno estratégico,
- factores regulatorios,
- capacidades institucionales,
- articulación con indicadores y objetivos institucionales.

**Lineamientos de Adopción y Articulación Institucional:** La revisión documental permitió evidenciar que los roles y responsabilidades asociados a la gestión del riesgo se encuentran definidos en el marco de las líneas de defensa establecidas en el documento PLE-PIN-M001 Manual de Gestión del Riesgo.

Así mismo, se evidenció que la Oficina Asesora de Planeación (OAP), como segunda línea de defensa, ejerce funciones de acompañamiento metodológico en las etapas de formulación, actualización y monitoreo de las matrices de riesgos de gestión.

En desarrollo de estas actividades, el Equipo de Riesgos de la OAP realiza revisión metodológica de los riesgos formulados por los líderes de proceso, verificando aspectos relacionados con:

- Coherencia entre el riesgo formulado y los objetivos del proceso.
- Identificación de causas asociadas a la materialización del riesgo.
- Definición de criterios de probabilidad e impacto.
- Estructuración metodológica de controles.
- Inclusión de atributos mínimos del control, tales como responsable, actividad de control, periodicidad y evidencia de ejecución.
- Lo anterior evidencia la existencia de mecanismos institucionales orientados a fortalecer la articulación metodológica de la gestión del riesgo bajo el esquema de líneas de defensa definido en MIPG y MECI.

**Monitoreo y Seguimiento:** En relación con las actividades de monitoreo y seguimiento, se evidenció que, de manera cuatrimestral, los equipos de trabajo de los procesos y las Alcaldías Locales consolidan y reportan información relacionada con la ejecución de controles asociados a los riesgos de gestión, así como las evidencias que soportan su aplicación durante el periodo evaluado.

La información es cargada en las carpetas institucionales definidas por la Oficina Asesora de Planeación, lo que permite mantener trazabilidad documental sobre las actividades de monitoreo adelantadas por la primera línea de defensa.

No obstante, durante la revisión efectuada se identifican oportunidades de fortalecimiento frente a:

- evaluación de efectividad de controles,
- monitoreo del riesgo residual,
- análisis de recurrencia de riesgos materializados,
- consolidación de indicadores clave de riesgo (KRI),
- seguimiento diferencial por tipología de riesgo.

**Presentación de Resultados y Custodia de la Información:** La revisión realizada permitió evidenciar que la Oficina Asesora de Planeación consolida y elabora informes relacionados con la gestión institucional del riesgo, los cuales son publicados en la página web de la Entidad como mecanismo de transparencia, divulgación y acceso a la información pública.

Así mismo, se evidenció que los resultados derivados de las actividades de monitoreo y seguimiento son presentados ante el Comité Institucional de Coordinación de Control Interno, instancia en la cual se socializan avances, observaciones y oportunidades de mejora relacionadas con la gestión integral del riesgo.

Lo anterior evidencia mecanismos institucionales orientados a fortalecer la gobernanza, trazabilidad y comunicación de la gestión del riesgo en el marco de las líneas de defensa y del Sistema de Control Interno.

En términos generales, se evidencian avances metodológicos y documentales en la implementación de la gestión de riesgos generales de gestión; no obstante, se identifican oportunidades de fortalecimiento relacionadas con la madurez institucional del sistema, particularmente en componentes asociados a monitoreo estratégico, evaluación de efectividad de controles, indicadores clave de riesgo, articulación territorial y consolidación del enfoque integral definido en la Guía para la Gestión Integral del Riesgo V7.

### 7.2.1.2. Caracterización de los riesgos generales de gestión

La Secretaría Distrital de Gobierno cuenta con 102 riesgos generales de gestión y 137 controles asociados, distribuidos en los diferentes procesos estratégicos, misionales, de apoyo, evaluación y mejora, y procesos transversales definidos dentro del mapa institucional de procesos.

Del total de riesgos identificados:

- el 23,5 % corresponde a procesos estratégicos, asociados principalmente a Planeación Institucional, Planeación y Gestión Sectorial, Gerencia TIC, Gestión del Patrimonio Documental y Comunicación Estratégica;
- el 32,4 % corresponde a procesos misionales, relacionados con Gestión Pública Territorial Local, Inspección, Vigilancia y Control, Acompañamiento a la Gestión Local, Relaciones Estratégicas, Convivencia y Diálogo Social, y Fomento y Protección de Derechos Étnicos y Derechos Humanos;
- el 37,3 % corresponde a procesos de apoyo, tales como Gestión Corporativa Institucional, Gestión del Talento Humano, Gestión Jurídica y Control Interno Disciplinario;
- el 4,9 % corresponde a procesos de evaluación y mejora;
- y el 1,9 % a procesos transversales asociados al Servicio a la Ciudadanía.

Lo anterior evidencia que la mayor concentración de riesgos se encuentra asociada a procesos de apoyo y misionales, lo cual resulta consistente con la complejidad operativa, administrativa y funcional de dichos procesos dentro de la cadena de valor institucional.

De los 19 mapas de riesgos revisados, se evidenció que 32 de los 102 riesgos identificados presentan alcance operativo en el Nivel Local. De estos:

- 10 corresponden al proceso de Inspección, Vigilancia y Control;
- 15 a Gestión Corporativa Institucional;
- 3 a Gestión Pública Territorial Local;
- y 4 a Acompañamiento a la Gestión Local.

Lo anterior evidencia participación del Nivel Local dentro de la gestión institucional del riesgo; no obstante, se identifican oportunidades de fortalecimiento frente a la incorporación de enfoques territoriales y diferenciales que permitan reflejar de manera más precisa las particularidades operativas, administrativas y de prestación del servicio de cada Alcaldía Local.

Tabla 3. Clasificación riesgos de gestión

CLASIFICACIÓN DEL PROCESO	CANT RIESGOS	CLASIFICACIÓN DEL RIESGO			CANT CONTROLES	TIPOLOGÍA DE CONTROLES		
		Ejecución y Administración de Procesos	Usuarios, productos y prácticas organizacionales	Ambiental		Preventivo	Detectivo	Correctivo
ESTRATÉGICO	24	20	0	4	29	14	12	3
MISIONAL	33	32	0	1	52	38	14	0
APOYO	38	24	1	13	46	25	18	3

CLASIFICACIÓN DEL PROCESO	CANT RIESGOS	CLASIFICACIÓN DEL RIESGO			CANT CONTROLES	TIPOLOGÍA DE CONTROLES		
		Ejecución y Administración de Procesos	Usuarios, productos y prácticas organizacionales	Ambiental		Preventivo	Detectivo	Correctivo
EVALUACIÓN Y MEJORA	5	5	0	0	7	3	4	0
TRANSVERSAL	2	2	0	0	3	2	0	1
<b>TOTAL</b>	<b>102</b>	<b>83</b>	<b>1</b>	<b>18</b>	<b>137</b>	<b>82</b>	<b>48</b>	<b>7</b>

Fuente: Elaboración propia OCI con base en reporte de la OAP

Del total de 102 riesgos generales de gestión identificados:

- el 81,3 % corresponde a riesgos asociados a ejecución y administración de procesos;
- el 17,6 % a riesgos de tipo ambiental;
- y el 0,9 % a riesgos asociados a usuarios, productos y prácticas organizacionales.

Lo anterior evidencia que la mayor exposición institucional se concentra en riesgos relacionados con la operación y ejecución de procesos, situación consistente con la naturaleza funcional, administrativa y operativa de la Entidad. Así mismo, se observa una participación relevante de riesgos de tipo ambiental, particularmente en procesos de apoyo y estratégicos, lo que evidencia la incorporación de factores asociados a condiciones del entorno, gestión institucional y sostenibilidad dentro de los ejercicios de identificación y valoración del riesgo. En cuanto a los controles asociados a riesgos generales de gestión, se identificaron 137 controles, de los cuales:

- el 59,8 % corresponde a controles preventivos;
- el 35,0 % a controles detectivos;
- y el 5,1 % a controles correctivos.

Lo anterior evidencia una mayor orientación institucional hacia mecanismos preventivos y de monitoreo, enfocados en disminuir la probabilidad de ocurrencia de los riesgos identificados y fortalecer la detección oportuna de desviaciones durante la operación de los procesos.

No obstante, la menor proporción de controles correctivos evidencia oportunidades de fortalecimiento frente a la capacidad institucional de respuesta, tratamiento y recuperación ante eventos de riesgo materializados, particularmente en aspectos relacionados con continuidad operativa, mitigación del riesgo residual y generación de acciones de mejora derivadas de incidentes o fallas de control.

Así mismo, durante la revisión efectuada se observó que los controles definidos en las matrices institucionales incorporan, en términos generales, atributos relacionados con responsable, actividad de control, periodicidad y evidencia de ejecución. Sin perjuicio de lo anterior, se identifican oportunidades de fortalecimiento frente a la evaluación de efectividad de controles, trazabilidad del monitoreo, articulación entre controles y causas raíz, así como en la definición de indicadores que permitan medir el comportamiento y evolución de los riesgos institucionales.

### 7.2.1.3. Identificación y descripción del riesgo

Para el desarrollo de la verificación y análisis de los riesgos generales de gestión, la Oficina de Control Interno seleccionó una muestra de siete (7) riesgos de un total de ciento dos (102) riesgos identificados, equivalente al 6,86 % del universo objeto de evaluación.

La selección de la muestra se realizó bajo un enfoque basado en riesgos y criterios de criticidad, priorizando riesgos clasificados en niveles extremo, alto y moderado, asociados a procesos estratégicos, misionales y de apoyo que presentan posibles afectaciones reputacionales, económicas y operacionales para la Entidad.

Los riesgos seleccionados corresponden a los procesos de:

- Comunicación Estratégica,
- Servicio a la Ciudadanía,
- Gestión Corporativa Institucional,
- Gestión Pública Territorial Local,
- Planeación y Gestión Sectorial,
- y Convivencia y Diálogo Social.

Sobre la muestra seleccionada se efectuó análisis metodológico de la formulación de los riesgos, verificando:

- claridad en la identificación del evento de riesgo,
- definición de causas inmediatas y causas raíz,
- identificación de consecuencias o impactos,
- coherencia entre riesgo, objetivo del proceso y controles asociados,
- y cumplimiento de los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo – Versión 7 de 2025.

Conforme a la Guía para la Gestión Integral del Riesgo V7, la adecuada formulación del riesgo debe contemplar, como elementos mínimos:

Tabla 4. Análisis identificación y descripción del riesgo de gestión

RIESGO FORMULADO	PROCESO	RIESGO INHERENTE	OBSERVACIÓN OCI
R1. Posibilidad de afectación reputacional por la pérdida de la integridad de la información relacionada con la gestión de la secretaría de gobierno en los medios de comunicación.	Comunicación Estratégica	Extremo	La formulación del riesgo identifica el impacto reputacional y el evento relacionado con la pérdida de integridad de la información; no obstante, no desarrolla de manera suficiente las causas inmediatas y causas raíz asociadas a la materialización del riesgo, lo que limita la trazabilidad metodológica requerida por la Guía V7 para la adecuada valoración y definición de controles.
R2: Posibilidad de afectación reputacional por la divulgación de información imprecisa, relacionada con la misionalidad de la Secretaría Distrital de Gobierno	Comunicación Estratégica	Extremo	Aunque el riesgo define el impacto reputacional y el evento asociado a la divulgación de información imprecisa, se identifican debilidades en la definición de factores causales relacionados con validación de contenidos, revisión de información y control de canales institucionales, afectando la precisión metodológica de la formulación.
R1. Posibilidad de afectación reputacional por la extemporaneidad en los tiempos de respuesta de acuerdo con los términos de la Ley 1755-2015 de los Derechos de Petición.	Servicio a la Ciudadanía	Alto	El riesgo describe el impacto reputacional derivado de la extemporaneidad en las respuestas; sin embargo, no incorpora de manera clara causas asociadas a seguimiento, capacidad operativa, gestión documental o controles de monitoreo, limitando la identificación integral de factores generadores del riesgo.
R1: Posibilidad de afectación reputacional por la suscripción de los contratos incumplimiento las normas contractuales, documentos y requisitos necesarios.	Gestión Corporativa Institucional - Nivel Central	Extremo	El riesgo presenta debilidades metodológicas y de redacción, dado que no diferencia claramente entre el evento y las causas del riesgo. Así mismo, requiere mejorar su estructura gramatical y precisar las posibles causas asociadas al incumplimiento normativo, tales como deficiencias en revisión jurídica, omisión de requisitos o debilidades en supervisión contractual. La guía recomienda formular riesgos claros, específicos y medibles.
R3. Posibilidad de afectación económica y reputacional por la inadecuada coordinación y articulación de la acción distrital en el territorio a través del Concejo Local de Gobierno	Gestión Pública Territorial Local	Moderado	El riesgo identifica los posibles impactos económicos y reputacionales; sin embargo, la formulación resulta ambigua respecto al evento de riesgo y no define claramente las causas asociadas a la inadecuada coordinación y articulación territorial. Conforme a la guía, la descripción del riesgo debe formularse con mayor precisión para facilitar la valoración de probabilidad e impacto y el diseño de controles efectivos.
R2: Afectación reputacional por lineamientos para la gestión del sector inoportunos y/o que no sean pertinentes	Planeación y Gestión Sectorial	Alto	La formulación describe el impacto reputacional y una condición asociada al riesgo; no obstante, no identifica claramente el evento ni las causas que originan la emisión de lineamientos inoportunos o no pertinentes. La guía establece que la formulación debe evitar términos ambiguos y describir de manera concreta el evento de riesgo, sus causas y consecuencias.
R1: Posibilidad de afectación reputacional y/o económica por el incumplimiento de acciones propias del programa de diálogo.	Convivencia y diálogo social	Alto	El riesgo identifica posibles impactos reputacionales y económicos; sin embargo, su formulación es general y no precisa las causas que pueden generar el incumplimiento de las acciones del programa, tales como falta de seguimiento, debilidades de planeación o insuficiencia de recursos. Conforme a la guía, los riesgos deben estructurarse de forma clara y específica para facilitar el monitoreo y la definición de controles.

Fuente: Elaboración propia OCI con base en reporte de la OAP

Del análisis realizado sobre la muestra evaluada, se evidenció que las principales oportunidades de fortalecimiento se concentran en la formulación metodológica de los riesgos, particularmente en aspectos relacionados con:

- identificación de causas inmediatas y causas raíz,
- precisión en la definición del evento de riesgo,
- diferenciación entre causas y consecuencias,
- y estructuración metodológica conforme a los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo V7.

Así mismo, se observó una alta concentración de riesgos orientados a impactos reputacionales, lo cual evidencia sensibilidad institucional frente a posibles afectaciones sobre la imagen, credibilidad y confianza en la gestión pública.

No obstante, en varios casos las formulaciones analizadas presentan un enfoque centrado principalmente en las consecuencias del riesgo, sin desarrollar suficientemente los factores causales y condiciones operativas que podrían generar su materialización, limitando la efectividad del análisis de probabilidad, la valoración del riesgo residual y la definición de controles preventivos y detectivos.

En consecuencia, se considera necesario fortalecer los ejercicios metodológicos de identificación y descripción del riesgo, promoviendo formulaciones más claras, específicas y trazables que faciliten la gestión integral del riesgo, el monitoreo y la toma de decisiones institucionales.

La OCI recomienda fortalecer las actividades de acompañamiento metodológico y revisión técnica adelantadas por la segunda línea de defensa, con el fin de mejorar la calidad y consistencia en la formulación de riesgos institucionales.

#### 7.2.1.4. Diseño y Análisis de Controles

Dando continuidad al análisis de los siete (7) riesgos seleccionados como muestra para la verificación, la Oficina de Control Interno efectuó revisión metodológica de los controles asociados, conforme a los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo – Versión 7 de 2025 y en el Manual de Gestión del Riesgo adoptado por la Entidad.

La evaluación contempló la verificación de la estructura metodológica de los controles, particularmente frente a la definición de:

- responsable de ejecución,
- actividad de control,
- periodicidad,
- manejo de desviaciones,
- y evidencias de ejecución, con el propósito de determinar su trazabilidad, coherencia y alineación frente a los riesgos formulados.

Tabla 5. Análisis identificación y descripción controles

ROCESO ASOCIADO / RIESGO	CONTROLES FORMULADOS	NATURALEZA DEL CONTROL	OBSERVACIÓN OCI
Comunicación Estratégica Riesgo 1	El jefe(a) de Oficina Asesora de Comunicaciones y el profesional de la oficina asignado realiza diariamente el seguimiento al monitoreo de medios, con el fin de detectar y dar oportuna rectificación de la noticia mal informada, si se da el caso. En caso de generarse una comunicación que afecte la gestión de la entidad se deberá desarrollar la estrategia inmediata de reacción. Como evidencia de la ejecución del control se realiza un informe de monitoreo por mes y se contará con 12 informes de monitoreo de medios en el año.	Detectivo	El control presenta una adecuada estructura metodológica, dado que identifica responsables, periodicidad, propósito del control, acción frente a desviaciones y evidencias de ejecución. Conforme a la guía, el control permite identificar elementos de seguimiento y trazabilidad; no obstante, se recomienda fortalecer indicadores de efectividad que permitan medir el impacto del control frente al riesgo reputacional identificado.
Comunicación Estratégica Riesgo 2	El profesional de la oficina de comunicaciones asignado revisa el Formato de Solicitud de Servicios de Comunicaciones (CES - F001), con base en la información de la solicitud elabora el contenido para la publicación, noticia, pieza gráfica o producto comunicativo. Previo a la publicación la información deberá ser verificada y confirmada por la dependencia que hizo el requerimiento. En caso de desviación se le deberá informar al líder del proceso mediante una comunicación escrita a través del correo institucional. Queda como evidencia del control, el formato de solicitud del servicio y la publicación final.	Preventivo	El control se encuentra alineado con los lineamientos de la guía, al establecer responsable, actividad de control, manejo de desviaciones y evidencias documentales. Así mismo, incorpora validación previa por parte de la dependencia solicitante, fortaleciendo el componente preventivo. Sin embargo, puede fortalecerse mediante la definición de criterios formales de validación y tiempos de revisión.
Servicio a la Ciudadanía Riesgo 1	El Profesional Especializado coordinador del grupo de Servicio de Atención a la Ciudadanía con apoyo de los funcionarios de los puntos de atención a la ciudadanía en Alcaldías locales y Nivel Central, realiza el seguimiento semanal de las respuestas a los Derechos de Petición, a través del aplicativo ORFEO. En caso de identificar respuestas sin cumplimiento de términos de tiempo establecidos, el Profesional Especializado del grupo de Servicio de Atención a la Ciudadanía generará alertas al responsable de la respuesta por medio de reuniones, comunicaciones a través de Teams o comunicaciones vía correo institucional. Como evidencia de la ejecución del control quedan soportes de reunión y/o comunicaciones a través de Microsoft Teams y el informe semanal al promotor de mejora de cada Alcaldía Local y Dependencia de Nivel Central, publicado en carpeta SharePoint.	Preventivo	El control presenta una estructura metodológica adecuada al definir responsable, periodicidad, mecanismo de seguimiento, acciones frente a desviaciones y evidencias del control. Se evidencia alineación con los criterios de la guía relacionados con monitoreo y trazabilidad; no obstante, se recomienda incluir indicadores de cumplimiento y tiempos de respuesta para medir la efectividad del control.
	El Profesional Especializado coordinador del Grupo de Servicio de Atención a la Ciudadanía realiza el seguimiento mensual a las respuestas de las peticiones de vigencias anteriores y actuales, a través del aplicativo BOGOTÁ TE ESCUCHA. En caso de identificar posibles desviaciones en la ejecución del control, se generarán las alertas en el informe mensual de seguimiento de cada alcaldía local y dependencias del Nivel Central, responsables funcionales de dar respuesta a los derechos de petición; con el fin de realizar la depuración y descongestión de los derechos de petición. Como evidencia de la ejecución del control se generan los informes mensuales de seguimiento a peticiones registradas en el aplicativo BOGOTÁ TE ESCUCHA.	Correctivo	El control cumple con varios criterios establecidos en la guía, toda vez que define periodicidad, responsables, acciones correctivas y evidencias documentales. Adicionalmente, incorpora mecanismos de alerta frente a posibles desviaciones. Sin embargo, se recomienda complementar con criterios de medición que permitan evaluar el nivel de reducción del riesgo.
Gestión Corporativa Institucional - Nivel Central Riesgo 1	En la fase de planeación, a solicitud del área que formula la necesidad de contratación, el director de Contratación designa a un profesional quien realiza acompañamiento en la construcción jurídica del proceso de selección, con el objetivo de adecuar el requerimiento a la normatividad vigente para la adquisición de que se trate. Como evidencia quedan los correos electrónicos o actas de reunión.	Preventivo	El control guarda coherencia con el riesgo identificado y establece responsable, propósito y evidencia. No obstante, la formulación puede fortalecerse incorporando periodicidad del control y criterios específicos de validación jurídica, conforme a la estructura sugerida en la guía.

	<p>Cada vez que se vaya a adelantar un proceso de selección, el director de Contratación ordena realizar el reparto a los profesionales considerando su experiencia y conocimientos. Como evidencia queda el registro en la matriz de reparto y en el aplicativo SIPSE.</p>	Preventivo	<p>El control presenta responsable, momento de ejecución y evidencia; sin embargo, la guía recomienda precisar criterios objetivos de asignación y mecanismos de seguimiento que permitan verificar la adecuada distribución de cargas y competencias.</p>
	<p>Cada vez que se adelanta un proceso de selección, en cualquier modalidad, cuenta con la revisión preliminar del gestor de contratación, el abogado asignado a cargo, y el flujo de revisión de la plataforma SECOP II que se compone de un abogado revisor y el director de Contratación. Como evidencia queda el flujo en el SIPSE y en el SECOP II.</p>	Preventivo	<p>El control se encuentra alineado con los lineamientos metodológicos de la guía, dado que define actividades de revisión, responsables y evidencias de trazabilidad. Adicionalmente, fortalece el principio de segregación de funciones y validación previa. Se recomienda complementar con criterios de seguimiento a observaciones o hallazgos identificados en las revisiones.</p>
Gestión Pública Territorial Local Riesgo 3	<p>La secretaría técnica del CLG cada vez que este convocada una sesión, verifica el quorum y en caso de no completarse el mismo levantará acta dejando constancia del hecho. El alcalde (sa) Local, en su calidad de presidente de la instancia enviará comunicaciones oficiales a los sectores integrantes informando la no realización de la sesión por falta de quorum. Igualmente, el alcalde Local comunicará al sector en caso de dificultades en la coordinación y articulación de los recursos. Las evidencias de la ejecución del control son las actas del CLG y las comunicaciones oficiales.</p>	Preventivo	<p>El control presenta responsables, acciones frente a desviaciones y evidencias documentales, alineándose con la estructura definida en la guía. No obstante, puede fortalecerse incorporando mecanismos de seguimiento sobre reincidencia de inasistencias o incumplimientos de articulación institucional.</p>
	<p>El Consejo Local de Gobierno elaborará el Plan Anual de trabajo de la instancia, de acuerdo con el procedimiento "GET-GPL-P001 Funcionamiento Consejo Local de Gobierno" establecido en el Sistema de Gestión de la entidad, verificando que se cumplan con los lineamientos establecidos. En caso de identificar alguna desviación en el cumplimiento de estos lineamientos se realizarán los respectivos ajustes al plan. Como evidencia de la ejecución del control queda el Plan de Trabajo Aprobado.</p>	Detectivo	<p>El control cumple parcialmente con los criterios metodológicos de la guía, al establecer actividad de validación y acciones de ajuste; sin embargo, requiere precisar responsables directos del seguimiento y mecanismos de monitoreo periódico sobre el cumplimiento del plan aprobado.</p>
Planeación y Gestión Sectorial – Riesgo 2	<p>La Oficina Asesora de Planeación, cada vez que se requiera, formula lineamientos que son presentados a las entidades del sector para retroalimentación y validación previo a su adopción por parte de las oficinas de planeación y/o del Comité Sectorial de Gestión y Desempeño, a través de reuniones de trabajo y/o comunicaciones oficiales establecidas en las entidades. En caso de no ser validados los lineamientos, se ajustarán y volverán a presentarlos hasta que se tome una decisión. Como soporte o trazabilidad queda las evidencias de las reuniones, comunicaciones oficiales, correos institucionales, y/o actas de Comité Sectorial de Gestión y Desempeño.</p>	Preventivo	<p>El control presenta una adecuada estructura al definir responsables, actividades de validación, acciones frente a desviaciones y soportes de trazabilidad. Conforme a la guía, el control fortalece la participación y retroalimentación previa a la adopción de lineamientos, aunque puede robustecerse mediante indicadores de pertinencia y oportunidad.</p>
	<p>El profesional asignado por el jefe de la OAP cada vez que ingresa un analista nuevo al proceso de Planeación y Gestión Sectorial, realiza la programación de una inducción en el puesto de trabajo y/o capacitación relacionada con lineamientos y metodologías para la gestión del sector. En caso de que no se pueda realizar la capacitación, se realizará una nueva programación. La evidencia de la aplicación de este control es el registro de capacitación, programación de las inducciones y Formato de entrenamiento en puesto de trabajo y demás soportes.</p>	Preventivo	<p>El control incorpora responsables, acciones y evidencias de ejecución; sin embargo, la guía recomienda definir periodicidad de seguimiento y mecanismos de evaluación que permitan verificar la efectividad de la capacitación impartida frente al riesgo identificado.</p>

<p>Convivencia y diálogo social Riesgo 1</p>	<p>El profesional encargado del apoyo a la coordinación de la línea de protesta de la dirección de convivencia y diálogo social o la persona designada por el líder del proceso, cada vez que ingrese un integrante nuevo al programa de diálogo social, debe realizar una capacitación de los temas del programa, normativa, funciones a desarrollar, documentos y formatos vigentes con su debido uso, para garantizar el conocimiento y funcionamiento del programa y posibilidad de cumplimiento de sus objetivos, y registrarlo en el formato DHH-CDS-F050 registro de encuentro, formación, capacitación, sensibilización y/o cualificación</p> <p>Así mismo, el equipo de fortalecimiento técnico y/o profesional delegado del equipo del observatorio, trimestralmente realiza una capacitación registrada en el formato DHH-CDS-F050 registro de encuentro, formación, capacitación, sensibilización y/o cualificación a los integrantes del programa para afianzar el conocimiento, uso de los documentos y formatos vigentes.</p> <p>En caso de evidenciar que no se ha realizado esta capacitación cada vez que ingrese un nuevo integrante al programa o de manera trimestral, se realiza la respectiva reprogramación.</p>	<p>Preventivo</p>	<p>El control presenta una estructura adecuada conforme a la guía, dado que incorpora responsables, periodicidad, acciones frente a desviaciones y evidencias documentales. Adicionalmente, fortalece la gestión del conocimiento y la prevención de errores operativos. No obstante, se recomienda incluir mecanismos de evaluación de aprendizaje y efectividad de las capacitaciones.</p>
	<p>El servidor público delegado por el director/a durante el desarrollo del evento realiza seguimiento de la información registrada en el aplicativo Poliscopio, garantizando que dicha información este debidamente registrada en cada apartado y en caso de identificar error del ingreso de información, se solicita a la persona que ingresa la información que realice el ajuste en su reporte</p> <p>Los servidores públicos designados por el director(a) de Convivencia y Diálogo Social de los equipos de la línea de Protesta, Observatorio de Conflictividad Social y profesional de la dirección, para hacer seguimiento en el aplicativo Poliscopio, dos veces al mes verifica la información registrada por parte de las personas en terreno. Como evidencia de la ejecución del control se registra el formato GDI-GPD-F029 evidencia de reunión, donde deben dejar registrado el resultado del contraste entre la sábana de datos exportada del aplicativo Poliscopio y los tableros publicados, en caso de encontrar inconsistencias en la información se solicita al observatorio de conflictividad social y/o equipo delegado realizar el ajuste en el aplicativo.</p> <p>Una vez al mes el profesional delegado del programa de diálogo y/u observatorio realiza una capacitación a servidores públicos que hicieron el registro con errores durante el periodo para que no se vuelva a repetir lo identificado. Como evidencia de la ejecución del control quedan los registros en el aplicativo de manera mensual, el formato DHH-CDS-F029 registro de acompañamiento y se registra en el formato DHH-CDS-F050 registro de encuentro, formación, capacitación, sensibilización y/o cualificación.</p>	<p>Detectivo</p>	<p>El control evidencia una adecuada estructura metodológica, incorporando responsables, periodicidad, validación de información, manejo de desviaciones y soportes documentales. Así mismo, incluye actividades de retroalimentación y capacitación correctiva, alineándose con los lineamientos de monitoreo y mejora continua establecidos en la guía.</p>

	<p>Los servidores públicos designados por parte del director de la DCDS para actividades locales del programa de diálogo social en la línea de cultura del diálogo mensualmente presentan el Formato plan de acción territorial DHH-CDS-F051 para realizar acciones de identificación y gestión territorial de conflictivos y promoción de la sana convivencia. El profesional designado por el director/a de la DCDS realiza seguimiento mensual y valida las actividades a realizar y en caso de no cumplir con los objetivos del programa retroalimenta para que se realice el ajuste o reprogramación, como evidencias de la ejecución del control se aporta GDI-GPD-F029 Formato Evidencia de Reunión con el plan de trabajo ajustado. Así mismo, el profesional designado por el director/a de DCDS de forma semestral realiza retroalimentación de las acciones en territorio y la estrategia al equipo de trabajo de la DCDS para que las acciones que se desarrollen en las localidades se hagan en el marco de las competencias y las registra como evidencia de uso del control el formato GDI-GPD-F029 Formato Evidencia de Reunión.</p>	<p>Preventivo</p>	<p>El control incorpora seguimiento periódico y mecanismos de retroalimentación sobre las acciones territoriales desarrolladas; no obstante, se identifican oportunidades de fortalecimiento relacionadas con indicadores de cumplimiento y evaluación del impacto de las acciones implementadas en territorio.</p>
	<p>El director cada vez que se solicite el acompañamiento del equipo del programa de diálogo verifica que estas actividades están en el marco de las competencias y objetivos del programa de diálogo, para lo cual cada dos semanas revisa y aprueba el acompañamiento solicitudes de otros eventos que tensionan la convivencia y registra la revisión como soporte de la ejecución del control en el formato GDI-GPD-F029 evidencia de reunión, de igual forma en caso de identificar que alguna solicitud de acompañamiento esta por fuera de las competencias, informa que no se acompaña el evento dejando como evidencia de ejecución del control correo electrónico, memorando u oficio.</p>	<p>Preventivo</p>	<p>El control fortalece mecanismos de validación frente a solicitudes de acompañamiento y verificación de competencias institucionales. Así mismo, incorpora evidencias documentales y actividades de revisión periódica; no obstante, puede fortalecerse mediante criterios formales de priorización y seguimiento de solicitudes rechazadas o no atendidas.</p>

Como resultado de la revisión efectuada sobre los controles asociados a la muestra seleccionada de riesgos generales de gestión, se evidenció que, en términos generales, los controles formulados presentan adecuada alineación con los criterios metodológicos establecidos en la Guía para la Gestión Integral del Riesgo – Versión 7 de 2025.

La mayoría de los controles evaluados incorporan elementos asociados a:

- responsables definidos,
  - periodicidad de ejecución,
  - actividades de seguimiento,
  - manejo de desviaciones,
  - y evidencias documentales,
- lo cual fortalece la trazabilidad y monitoreo de los riesgos institucionales.

Así mismo, se observó predominio de controles orientados a:

- seguimiento operativo,
- validación de información,
- monitoreo normativo,
- capacitación,
- revisión documental,

- y actividades preventivas y detectivas, permitiendo evidenciar mecanismos institucionales orientados a la mitigación y monitoreo de riesgos.

No obstante, durante el análisis realizado se identificaron oportunidades de fortalecimiento relacionadas con:

- definición de indicadores de efectividad,
- evaluación del impacto del control sobre el riesgo residual,
- simplificación y estandarización de controles,
- definición de criterios objetivos de medición,
- y consolidación de mecanismos de seguimiento orientados a la mejora continua.

Adicionalmente, se evidenció que algunos controles incorporan múltiples actividades dentro de una misma formulación, situación que podría dificultar su monitoreo individual, trazabilidad y evaluación de efectividad.

En consecuencia, se recomienda fortalecer la evaluación periódica de efectividad de controles y avanzar en la implementación de indicadores asociados al comportamiento del riesgo y la reducción del riesgo residual, conforme al enfoque de mejora continua y monitoreo definido en la Guía V7.

#### 7.2.1.5. Análisis de Riesgo Inherente vs. Riesgo Residual

A continuación, se presentan los resultados del análisis comparativo entre la valoración del riesgo inherente y el riesgo residual de los riesgos generales de gestión identificados por la Entidad, con el propósito de evaluar el comportamiento del riesgo posterior a la aplicación de controles y el tratamiento definido para cada proceso.

El análisis fue realizado sobre los diecinueve (19) mapas de riesgos de gestión aportados por la Oficina Asesora de Planeación, considerando:

- nivel de criticidad,
- valoración inherente,
- controles asociados,
- valoración residual,
- y tratamiento del riesgo.

Tabla 6. Valoración riesgo inherente Vrs. Riesgo Residual

TIPO DE PROCESO	PROCESO	CANTIDAD DE RIESGOS	CALIFICACIÓN RIESGO INHERENTE				CANTIDAD DE CONTROLES	CALIFICACIÓN RIESGO RESIDUAL				TRATAMIENTO		
			EXT	ALT	MOD	BAJ		EXT	ALT	MOD	BAJ	ACE	RED	ELI
ESTRATÉGICO	Planeación Institucional	5	0	0	4	1	6	0	0	3	3	6	0	0
	Planeación y Gestión Sectorial	3	0	2	1	0	5	0	2	2	1	5	0	0
	Gerencia De Tic	7	0	0	4	3	8	0	0	3	5	4	0	0

TIPO DE PROCESO	PROCESO	CANTIDAD DE RIESGOS	CALIFICACIÓN RIESGO INHERENTE				CANTIDAD DE CONTROLES	CALIFICACIÓN RIESGO RESIDUAL				TRATAMIENTO		
			EXT	ALT	MOD	BAJ		EXT	ALT	MOD	BAJ	ACE	RED	ELI
	Gestión Del Patrimonio Documental	5	0	2	1	2	6	0	2	1	3	6	0	0
	Comunicación Estratégica	4	2	0	2	0	4	2	0	2	0	4	0	0
MISIONAL	Gestión Pública Territorial Local	3 <u>Alcance NL</u>	0	0	3	0	5	0	0	5	0	5	0	0
	Inspección, Vigilancia y Control	10 <u>Alcance NL</u>	0	3	7	0	12	0	1	11	0	12	0	0
	Acompañamiento A La Gestión Local	4 <u>Alcance NL</u>	0	0	2	2	5	0	0	2	3	5	0	0
	Relaciones Estratégicas	6	0	1	4	1	6	0	0	5	1	6	0	0
	Convivencia y Dialogo Social	4	0	1	3	0	15	0	0	15	0	4	0	0
	Fomento Y Protección De Los Derechos Humanos	5	0	0	0	5	8	0	0	0	8	8	0	0
	Fomento Y Protección De Los Derechos Étnicos	1	0	0	0	1	1	0	0	0	1	1	0	0
	Gestión Jurídica	3	0	1	2	0	5	0	1	4	0	5	0	0
APOYO	Gestión Corporativa Institucional	11	1	2	8	0	13	1	1	6	5	10	3	0
		15 <u>Alcance NL</u>	0	5	8	2	18	0	3	11	4	16	2	0
	Gerencia Del Talento Humano	7	0	0	4	3	8	0	0	4	4	8	0	0
	Control Disciplinario	2	0	0	2	0	2	0	0	2	0	0	2	0
EVALUACIÓN Y MEJORA	Gestión Del Conocimiento	4	0	0	2	2	4	0	0	2	2	4	0	0
	Evaluación Independiente	1	0	0	1	0	3	0	0	1	2	3	0	0
TRANSVERSAL	Servicio a la Ciudadanía	2	0	2	0	0	3	0	1	2	0	1	2	0

TIPO DE PROCESO	PROCESO	CANTIDAD DE RIESGOS	CALIFICACIÓN RIESGO INHERENTE				CANTIDAD DE CONTROLES	CALIFICACIÓN RIESGO RESIDUAL				TRATAMIENTO		
			EXT	ALT	MOD	BAJ		EXT	ALT	MOD	BAJ	ACE	RED	ELI
	19 mapas de riesgos	102	3	19	58	22	137	3	11	81	42	113	9	0

Fuente: Elaboración propia OCI con base en reporte de la OAP

Del total de 102 riesgos evaluados en su valoración inherente:

- 3 riesgos (2,9 %) se clasifican en zona extrema;
- 19 (18,6 %) en zona alta;
- 58 (56,9 %) en zona moderada;
- y 22 (21,6 %) en zona baja.

Lo anterior evidencia una mayor concentración institucional en niveles moderados de riesgo; no obstante, persisten riesgos clasificados en zonas de criticidad extrema y alta asociados a procesos estratégicos, misionales y de apoyo, los cuales requieren especial monitoreo y fortalecimiento de controles.

El análisis comparativo entre el riesgo inherente y el riesgo residual permite identificar el comportamiento del nivel de exposición al riesgo posterior a la aplicación de controles, así como evaluar la capacidad de mitigación de las medidas implementadas por los diferentes procesos de la Entidad.

A partir de este análisis se evidenció:

- La totalidad de los riesgos clasificados inicialmente en zona extrema (3) mantuvo la misma valoración residual posterior a la aplicación de controles, correspondiendo a los procesos de Comunicación Estratégica y Gestión Corporativa Institucional. Lo anterior evidencia que, aunque los controles implementados incorporan actividades preventivas y de monitoreo, estos no generan reducción suficiente en la severidad residual del riesgo conforme a la metodología de valoración aplicada por la Entidad.
- En el proceso de Comunicación Estratégica se evaluaron riesgos asociados a posibles afectaciones reputacionales derivadas de pérdida de integridad y divulgación de información imprecisa relacionada con la gestión institucional. Los controles implementados se orientan principalmente al monitoreo de medios, validación de contenidos y verificación previa de información; no obstante, la valoración residual permanece en zona extrema, situación que evidencia oportunidades de fortalecimiento frente a la capacidad de mitigación del riesgo reputacional y al seguimiento de la efectividad de los controles implementados
- Para el proceso de Gestión Corporativa Institucional se analizó el riesgo asociado a la suscripción de contratos incumpliendo normas y requisitos contractuales. Aunque se evidenciaron controles relacionados con acompañamiento jurídico, asignación de procesos y revisión mediante SIPSE y SECOP II, el riesgo residual continúa en zona extrema, evidenciando la necesidad de fortalecer la efectividad de los controles y revisar su valoración residual conforme a la Guía para la Gestión Integral del Riesgo V7. En caso de materializarse, la entidad podría enfrentar hallazgos administrativos, disciplinarios y fiscales, posibles demandas, nulidad de contratos, retrasos en la ejecución contractual y afectación reputacional e institucional.

- De los diecinueve (19) riesgos clasificados como altos en el riesgo inherente, nueve (9) se mantienen en la misma categoría en el riesgo residual. Estos corresponden a los procesos de Gestión del Patrimonio Documental (2), Inspección, Vigilancia y Control (1), Gestión Jurídica (1), Gestión Corporativa Institucional (4) y Servicio a la Ciudadanía (1). – Los riesgos clasificados en zonas de mayor criticidad (extrema y alta) se relacionan principalmente con:
  - **Incumplimiento normativo y contractual**, especialmente en procesos de contratación, derivado de desconocimiento de la normatividad, debilidades en revisión jurídica y deficiencias en la aplicación de requisitos contractuales.
  - **Afectación reputacional por divulgación o manejo inadecuado de información**, asociada a fallas en comunicación institucional, lineamientos inoportunos y deficiencias en validación de contenidos.
  - **Incumplimiento en tiempos de respuesta a la ciudadanía**, particularmente frente a derechos de petición y atención ciudadana, asociado a debilidades operativas, gestión documental y funcionamiento de aplicativos institucionales.
  - **Debilidades en articulación y coordinación territorial**, relacionadas con baja participación ciudadana, deficiencias en coordinación interinstitucional y dificultades en la formulación y gestión de proyectos locales.
  - **Deficiencias en seguimiento y ejecución de programas institucionales**, especialmente en programas de diálogo social, formulación de políticas públicas y acciones territoriales.
  - **Riesgos ambientales y operacionales**, asociados a manejo inadecuado de residuos peligrosos, almacenamiento de sustancias, mantenimiento del parque automotor y cumplimiento de lineamientos ambientales.
- Como resultado de la aplicación de controles y la valoración residual efectuada en las matrices institucionales, se observó disminución en el nivel de criticidad en 10 de los 22 riesgos clasificados inicialmente en zonas extrema y alta, equivalente al 45 % de los riesgos evaluados en dichas categorías.

El análisis realizado evidencia oportunidades de fortalecimiento en el diseño, implementación y monitoreo de los controles asociados a riesgos críticos, particularmente en aquellos casos donde la valoración residual permanece en zonas extrema y alta posterior a la aplicación de controles.

Así mismo, se identificó una alta concentración de tratamientos orientados a la aceptación del riesgo (92,6 %), frente a una menor proporción de estrategias orientadas a reducción o mitigación (7,3 %).

Lo anterior evidencia necesidad de fortalecer el análisis institucional frente a criterios de apetito, tolerancia y capacidad de respuesta al riesgo, promoviendo estrategias de tratamiento orientadas a disminuir la probabilidad e impacto de riesgos críticos, particularmente aquellos asociados a afectaciones económicas, jurídicas, operacionales y reputacionales.

#### 7.2.1.6. Resultados del Monitoreo

El Manual de Gestión del Riesgo PLE-PIN-M001 Versión 9 establece que las actividades de monitoreo y seguimiento de los riesgos de gestión deben desarrollarse bajo el esquema de líneas de defensa definido en el Modelo Integrado de Planeación y Gestión – MIPG, asignando responsabilidades diferenciadas a la primera, segunda y tercera línea de defensa.

En este marco:

- la primera línea de defensa, conformada por líderes de proceso y Alcaldías Locales, es responsable del monitoreo permanente de riesgos, ejecución de controles, identificación de riesgos materializados y seguimiento a acciones de mejora;
- la segunda línea de defensa, a cargo de la Oficina Asesora de Planeación, realiza acompañamiento metodológico, monitoreo independiente y seguimiento a la gestión del riesgo;
- y la tercera línea de defensa, correspondiente a la Oficina de Control Interno, efectúa evaluación independiente sobre la efectividad del sistema de gestión del riesgo y sus mecanismos de control.

La Oficina de Control Interno recibió por parte de la Oficina Asesora de Planeación tres informes cuatrimestrales correspondientes a la vigencia 2025, en los cuales se consolidan los resultados del monitoreo efectuado a los riesgos de gestión y corrupción del Nivel Central y Nivel Local.

De acuerdo con la información reportada, durante la vigencia se materializaron dieciocho (18) riesgos, de los cuales dieciséis (16) corresponden a riesgos de gestión y dos (2) a riesgos de corrupción.

A continuación, se presenta la relación de los riesgos de gestión materializados durante la vigencia:

Tabla 7. Relación riesgos de gestión materializados

CUATRIMESTRE 2025	NIVEL	CANT	IMPLEMENTO PLAN DE ACCIÓN		TOTAL, RIESGOS MATERIALIZADOS POR CUATRIMESTRE
			SÍ	NO	
1er Cuatrimestre	Central	3	3	-	5
	Local	2	-	2	
2do Cuatrimestre	Central	2	2	-	8
	Local	6	-	6	
3er Cuatrimestre	Central	2	1	1	3
	Local	1	0	1	
<b>TOTAL, RIESGOS MATERIALIZADOS</b>		<b>16</b>	<b>6</b>	<b>10</b>	<b>16</b>

Fuente: Elaboración propia OCI con base en reporte de la OAP

De los dieciséis (16) riesgos materializados durante la vigencia 2025, el 61,1 % (10 riesgos) corresponde al Nivel Local y el 38,9 % (6 riesgos) al Nivel Central.

Así mismo, se evidenció que únicamente seis (6) riesgos materializados cuentan con planes de acción implementados, mientras que en los demás casos no se observó reporte de acciones de tratamiento o seguimiento asociadas a la materialización del riesgo.

Lo anterior evidencia oportunidades de fortalecimiento frente al cumplimiento de las directrices institucionales relacionadas con el tratamiento, seguimiento y monitoreo de riesgos materializados

A continuación, se presenta de manera detallada la relación de los riesgos materializados por proceso, tanto en el Nivel Central como en el Nivel Local, así como la identificación de aquellos riesgos que han presentado recurrencia.

Tabla 8. Relación riesgos de gestión materializados Nivel Central

RIESGOS MATERIALIZADOS - NIVEL CENTRAL			
CUATRIMESTRE	PROCESO	RIESGO	PLAN DE MEJORAMIENTO ASOCIADO
1ER CUATRIMESTRE	Relaciones Estratégicas	R3	475
	Relaciones Estratégicas	R4	475
	Servicio al Ciudadano Transversal NC - NL	R1	498
2DO CUATRIMESTRE	Servicio al ciudadano Transversal NC -NL	R1	Del 479 al 548 correspondientes a 19 alcaldías locales
	Relaciones estratégicas	R3	475
3ER CUATRIMESTRE	Servicio a la Ciudadanía Transversal NC - NL	R1	30 planes de acción asociados, con alcance a todas las Alcaldías Locales
	Planeación Institucional	R3	No reportan plan de mejora
<b>TOTAL, RIESGOS MATERIALIZADOS</b>		<b>7</b>	

Fuente: Elaboración propia OCI con base en reporte de la OAP

Tabla 9. Relación riesgos de gestión materializados Nivel Local

RIESGOS MATERIALIZADOS - NIVEL LOCAL				
CUATRIMESTRE	PROCESO	ALCALDÍA	RIESGO	PLAN DE MEJORAMIENTO ASOCIADO
1ER CUATRIMESTRE	Gestión Pública Territorial Local	Bosa	R3	No reportan formulación de plan de mejoramiento
	Gestión Pública Territorial Local	Bosa	R5	No reportan formulación de plan de mejoramiento.
2DO CUATRIMESTRE	Gestión Corporativa Institucional	Santafé	R09	No relacionan número de plan de mejora formulada.
	Gestión Corporativa Institucional	Santafé	R12	No relacionan número de plan de mejora formulada.
	Gestión Pública Territorial Local	Bosa	R3	Durante los 2 primeros cuatrimestres y no se generan planes de mejoramiento
	Inspección, Vigilancia y Control	Bosa	R7	No relacionan número de plan de mejora formulada.
	Gestión Corporativa Institucional	Fontibón	R8	No relacionan número de plan de mejora formulada.
	Gestión Corporativa Institucional	Fontibón	R11	No relacionan número de plan de mejora formulada.
3ER CUATRIMESTRE	Gestión Corporativa Institucional	Bosa	R12	No reportan plan de mejora Interno
<b>TOTAL</b>			<b>9 RIESGOS</b>	

Fuente: Elaboración propia OCI con base en reporte de la OAP

- **Riesgos con materialización recurrente:**

Durante los tres ciclos de monitoreo efectuados se evidenció recurrencia en la materialización de tres (3) riesgos asociados a los procesos de Relaciones Estratégicas, Servicio a la Ciudadanía y Gestión Pública Territorial Local – Alcaldía Local de Bosa.

La recurrencia observada evidencia oportunidades de fortalecimiento frente al tratamiento, seguimiento y monitoreo de riesgos previamente identificados, así como frente a la implementación y evaluación de acciones orientadas a evitar la repetición de eventos de riesgo materializados.

A continuación, se detallan los riesgos materializados que han presentado recurrencia durante el año 2025:

Tabla 10. Relación riesgos materializados con mayor recurrencia

RIESGO	NO. RIESGO	PROCESO / ALCADÍA	OBSERVACIÓN OCI
Posibilidad de afectación reputacional por la inoportuna atención de las dependencias internas de la SDG a las respuestas de los derechos de petición solicitadas por las corporaciones de elección popular.	R3	Relaciones Estratégicas	Durante el primer y segundo cuatrimestre se evidenció materialización del riesgo. Se observó formulación del plan de acción No. 475; no obstante, persiste recurrencia del evento durante la vigencia evaluada.
Posibilidad de afectación reputacional por la extemporaneidad en los tiempos de respuesta de acuerdo con los términos de la Ley 1755-2015 de los Derechos de Petición.	R1	Servicio a la ciudadanía NC/ 20 AL	1 riesgo presentó materialización durante los tres cuatrimestres evaluados. Se evidenció formulación de treinta (30) planes de acción asociados al Nivel Central y Alcaldías Locales, de los cuales quince (15) registran estado “Cerrado” y quince (15) estado “Abierto” en la plataforma MIMEC.
GPL: Posibilidad de afectación económica y reputacional por la inadecuada coordinación y articulación de la acción distrital en el territorio a través del Concejo Local de Gobierno	R3	Gestión Pública Territorial Local <u>ALBOSA</u>	El riesgo se materializó durante el primer y segundo cuatrimestre. No se evidenció reporte de planes de acción asociados en la información suministrada, situación que limita el seguimiento y tratamiento frente al evento materializado.

Fuente: Elaboración propia OCI con base en reporte de la OAP

En términos generales, el análisis de los riesgos materializados durante la vigencia 2025 evidencia recurrencia principalmente en riesgos asociados a:

- oportunidad en la atención de derechos de petición,
- coordinación institucional,
- articulación territorial,
- y seguimiento de acciones operativas.
- 

Se observó que el proceso de Servicio a la Ciudadanía presenta el mayor número de eventos materializados y de planes de acción asociados, tanto en el Nivel Central como en las Alcaldías Locales.

Así mismo, durante la revisión realizada se identificaron oportunidades de fortalecimiento frente a:

- seguimiento de riesgos materializados,

- implementación de acciones de mejora,
- cierre efectivo de planes asociados,
- monitoreo del riesgo residual,
- y evaluación de efectividad de controles.

No obstante, pese a que varios planes asociados al riesgo R1 registran estado “Cerrado” en la plataforma MIMEC, se evidenció continuidad en la materialización del riesgo durante diferentes periodos de seguimiento, situación que evidencia necesidad de fortalecer el análisis de causas, el seguimiento a controles implementados y la evaluación de efectividad de las acciones formuladas.

De igual manera, para el riesgo R3 del proceso Gestión Pública Territorial Local – Alcaldía Local de Bosa, materializado durante el primer y segundo cuatrimestre, no se evidenció reporte de planes de mejoramiento asociados, limitando la definición y seguimiento de acciones orientadas al tratamiento del evento materializado.

Lo anterior cobra relevancia considerando que la Guía para la Gestión Integral del Riesgo V7 establece la necesidad de:

- analizar las causas asociadas a riesgos materializados,
- evaluar la efectividad de los controles implementados,
- definir acciones de tratamiento,
- realizar seguimiento continuo,
- y fortalecer mecanismos de mitigación orientados a prevenir recurrencia de eventos de riesgo.

En consecuencia, la recurrencia observada en algunos riesgos materializados, junto con las oportunidades de mejora identificadas en materia de seguimiento, monitoreo y formulación de acciones de tratamiento, evidencia necesidad de fortalecer componentes asociados a la gestión integral del riesgo, particularmente frente a:

- monitoreo de riesgos materializados,
- efectividad de controles,
- seguimiento a planes de acción,
- y evaluación del riesgo residual, con el fin de mejorar la capacidad institucional de prevención y respuesta frente a eventos de riesgo.

La OCI recomienda fortalecer los mecanismos de seguimiento y monitoreo de riesgos materializados, incorporando análisis de causas, evaluación periódica de efectividad de controles y trazabilidad sobre el cumplimiento de los planes de acción implementados.

## **7.2.2. Gestión de Riesgos de Seguridad de la Información.**

### **7.2.2.1. Herramientas para la gestión del riesgo**

La Secretaría Distrital de Gobierno cuenta con instrumentos metodológicos y documentales orientados a la gestión de riesgos de seguridad de la información, los cuales incorporan lineamientos definidos en la Guía para la Gestión Integral del Riesgo – Versión 7 de 2025 y elementos asociados al Modelo de Seguridad y Privacidad de la Información (MSPI).

La gestión de los riesgos de seguridad de la información se desarrolla mediante herramientas institucionales orientadas a la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de riesgos asociados a la disponibilidad, integridad y confidencialidad de la información institucional.

- **Documentación Relacionada**

Para la administración de los riesgos de seguridad de la información, la entidad dispone de la siguiente documentación:

Código	Documento	Versión
PLE-PIN-M001	Manual de Gestión del Riesgo	09

En el numeral 13 “Lineamientos Riesgos de Seguridad de la Información” del Manual de Gestión del Riesgo PLE-PIN-M001 Versión 09, se establece la articulación de la política de seguridad digital con el Modelo de Seguridad y Privacidad de la Información (MSPI), alineándola con el Marco de Referencia de Arquitectura TI y los habilitadores de la Política de Gobierno Digital relacionados con: seguridad de la información, arquitectura institucional y servicios ciudadanos digitales.

Lo anterior evidencia incorporación institucional de lineamientos asociados a seguridad digital y gestión de riesgos tecnológicos dentro del marco metodológico de administración del riesgo.

La Entidad dispone de dieciocho (18) matrices de riesgos de seguridad de la información, distribuidas así:

- trece (13) matrices correspondientes a procesos del Nivel Central;
- cinco (5) matrices correspondientes a Alcaldías Locales.

Durante la revisión realizada se evidenció que las matrices de riesgos de seguridad de la información se encuentran en proceso de construcción y ajuste metodológico, razón por la cual aún no cuentan con formalización documental mediante fecha de aprobación o control de versiones.

No obstante, el modelo de matriz utilizado por la Entidad incorpora elementos metodológicos orientados a:

- identificación del riesgo,
- amenazas,
- vulnerabilidades,
- controles,
- valoración inherente y residual,
- planes de tratamiento,
- monitoreo,
- responsables,
- evidencias,
- indicadores.

**Análisis de Contexto y DOFA:** De acuerdo con la información revisada, las matrices de riesgos de seguridad de la información incorporan metodológicamente componentes asociados al análisis de contexto y matriz

DOFA; no obstante, dichos elementos aún se encuentran en proceso de construcción y consolidación en las matrices aportadas para análisis.

**Lineamientos de Adopción y Articulación Institucional:** Se evidenció que la Dirección de Tecnologías e Información (DTI), a través del equipo de Seguridad de la Información, realiza acompañamiento metodológico a dependencias y Alcaldías Locales en la formulación de matrices de riesgos de seguridad de la información, ejerciendo funciones asociadas a la segunda línea de defensa frente a riesgos tecnológicos y de seguridad digital.

Así mismo, el Manual de Gestión del Riesgo establece la articulación de estos riesgos con el Modelo de Seguridad y Privacidad de la Información (MSPI), fortaleciendo la gestión institucional frente a amenazas tecnológicas, vulnerabilidades y riesgos asociados a seguridad digital.

**Monitoreo y Seguimiento:** El monitoreo de riesgos y controles asociados a seguridad de la información se desarrolla mediante el formato institucional PLE-PIN-F042 “Formato Matriz de Riesgos de Seguridad de la Información”, el cual incorpora elementos orientados al seguimiento y actualización periódica de riesgos tecnológicos.

Conforme al procedimiento PLE-PIN-P017, el monitoreo de riesgos de seguridad de la información debe realizarse al menos una vez al año por cada dependencia y Alcaldía Local, con acompañamiento de la Dirección de Tecnologías e Información – equipo de Seguridad de la Información.

Así mismo, la DTI participa en la evaluación de planes de tratamiento y en la actualización de la valoración de riesgos, mientras que las dependencias y Alcaldías Locales son responsables de verificar la implementación y operación de los controles definidos.

**Presentación de Resultados y Custodia de la Información:** El procedimiento PLE-PIN-P017 establece que, una vez aprobadas las matrices de riesgos de seguridad de la información por parte de cada jefe de dependencia o Alcalde Local, estas deben ser almacenadas en los repositorios definidos por la Dirección de Tecnologías e Información – equipo de Seguridad de la Información.

Debido a la sensibilidad de la información contenida en dichas matrices, estas no son objeto de publicación institucional, en aplicación de criterios de reserva y protección de información asociados a seguridad digital.

Así mismo, la Dirección de Tecnologías e Información consolida institucionalmente los riesgos de seguridad de la información y presenta periódicamente los resultados ante el Comité Institucional de Gestión y Desempeño, como mecanismo de seguimiento y gobernanza institucional frente a riesgos tecnológicos.

En términos generales, se evidencian avances institucionales en la estructuración metodológica para la gestión de riesgos de seguridad de la información, particularmente frente a la incorporación de lineamientos asociados al MSPI y a la definición de herramientas para identificación y tratamiento de riesgos tecnológicos.

No obstante, se identifican oportunidades de fortalecimiento relacionadas con:

- formalización documental de matrices,
- consolidación metodológica del análisis de contexto,
- ampliación del alcance en el Nivel Local,
- definición de indicadores de efectividad,

- y fortalecimiento del monitoreo y seguimiento de riesgos tecnológicos y de seguridad digital.

#### 7.2.2.2. Caracterización de los riesgos de seguridad de la información:

La Secretaría Distrital de Gobierno cuenta con 68 riesgos de seguridad de la información y 180 controles asociados.

Del total de riesgos identificados:

- el 7,5 % corresponde a procesos estratégicos;
- el 22,0 % a procesos misionales;
- el 17,6 % a procesos de apoyo;
- el 2,9 % a procesos de evaluación y mejora y procesos transversales;
- el 50 % restante corresponde a riesgos identificados en el Nivel Local.

De los 18 mapas de riesgos revisados, 34 riesgos corresponden al Nivel Local, distribuidos en las Alcaldías Locales de:

- Barrios Unidos,
- San Cristóbal,
- Engativá,
- Puente Aranda,
- Teusaquillo.

Lo anterior evidencia una implementación parcial del modelo de riesgos de seguridad de la información en las Alcaldías Locales.

Así mismo, se identificó que:

- el 48,5 % de los riesgos se encuentra asociado al principio de disponibilidad;
- el 30,8 % a integridad;
- el 20,5 % a confidencialidad.

En relación con los controles, el 84,4 % corresponde a controles preventivos y el 15,6 % a controles detectivos, evidenciando una orientación institucional enfocada principalmente en la prevención y mitigación temprana de riesgos asociados a seguridad digital y continuidad operativa.

Tabla 11. Caracterización riesgos de seguridad de la información

TIPO PROCESO	CANT RIESGOS	PRINCIPIO DE SEGURIDAD			CANT CONTROLES	TIPOLOGÍA DEL CONTROL	
		Disponibilidad	Integridad	Confidencialidad		Preventivo	Detectivo
ESTRATÉGICO	5	2	3	0	8	6	2
MSIONAL	15	6	8	1	46	40	6
APOYO	12	7	3	2	28	26	2

TIPO PROCESO	CANT RIESGOS	PRINCIPIO DE SEGURIDAD			CANT CONTROLES	TIPOLOGÍA DEL CONTROL	
		Disponibilidad	Integridad	Confidencialidad		Preventivo	Detectivo
EVALUACIÓN Y MEJORA	1	0	1	0	2	2	0
TRANSVERSAL	1	0	1	0	6	6	0
NIVEL LOCAL	34	18	5	11	90	72	18
<b>TOTAL</b>	<b>68</b>	33	21	14	<b>180</b>	152	28

Fuente: Elaboración OCI con la información aportada por DTI

De acuerdo con la revisión realizada sobre la información aportada por la Dirección de Tecnologías e Información – DTI, se evidenció que no todas las dependencias y Alcaldías Locales cuentan con matrices de riesgos de seguridad de la información identificadas y formalizadas, pese a que el Manual PLE-PIN-M001 Versión 09 establece lineamientos generales para su aplicación en procesos del Nivel Central y Nivel Local.

Así mismo, se identificó que algunas dependencias estratégicas y de apoyo relacionadas con: gestión documental, tecnologías de la información, comunicaciones, gestión del conocimiento, no evidenciaron matrices específicas de riesgos de seguridad de la información dentro de la documentación suministrada, situación que podría afectar la identificación integral de amenazas, vulnerabilidades y riesgos asociados a disponibilidad, integridad, confidencialidad y trazabilidad de la información institucional.

De acuerdo con las matrices aportadas por la Dirección de Tecnologías e Información – DTI, no se evidenció identificación ni formulación de riesgos de seguridad de la información para las siguientes dependencias y procesos institucionales

Tabla 12. Riesgos de Seguridad de la Información Nivel Central

DEPENDENCIA / DIRECCIÓN	PROCESO ASOCIADO	OBSERVACIÓN
Despacho Secretaría Distrital de Gobierno	Relaciones Estratégicas	De acuerdo con las matrices aportadas por la Dirección de Tecnologías e Información – DTI, no se evidenció identificación ni formulación de riesgos de Seguridad de la Información para las dependencias y procesos relacionados.
Oficina Asesora de Comunicaciones	Comunicación Estratégica	
Dirección de Tecnología e Información	Gerencia de Tecnología e Información (TIC)	
Dirección de Gestión Documental	Gestión Patrimonio Documental	
Dirección de Inspección, Vigilancia y Control	Inspección, Vigilancia y Control	
Alcaldías Locales	Gestión Corporativa Institucional – NL	
Dependencia de Gestión del Conocimiento	Gestión del Conocimiento	

Fuente: Elaboración OCI con la información aportada por DTI

Se observó que únicamente cinco (5) Alcaldías Locales evidenciaron matrices de riesgos de seguridad de la información, situación que evidencia una implementación parcial del modelo institucional de gestión de riesgos de seguridad de la información y limita su cobertura integral en el Nivel Local.

En consecuencia, se identifican oportunidades de fortalecimiento frente a la formulación e implementación de riesgos de seguridad de la información en las demás Alcaldías Locales, conforme a los lineamientos definidos en el Manual PLE-PIN-M001 V9 y la Guía para la Gestión Integral del Riesgo V7.

Tabla 13. Riesgos de Seguridad de la Información Nivel Local

Alcaldía Local	Observación
Alcaldía Local de Antonio Nariño	No se cuenta con identificación y formulación de riesgos de Seguridad de la Información, de acuerdo con las matrices aportadas por la Dirección de Tecnologías e Información – DTI.
Alcaldía Local de Bosa	
Alcaldía Local de Chapinero	
Alcaldía Local de Ciudad Bolívar	
Alcaldía Local de Fontibón	
Alcaldía Local de Kennedy	
Alcaldía Local de La Candelaria	
Alcaldía Local de Los Mártires	
Alcaldía Local de Rafael Uribe Uribe	
Alcaldía Local de Santa Fe	
Alcaldía Local de Suba	
Alcaldía Local de Sumapaz	
Alcaldía Local de Tunjuelito	
Alcaldía Local de Usaquén	
Alcaldía Local de Usme	

Fuente: Elaboración OCI con la información aportada por DTI

La revisión efectuada evidencia oportunidades de fortalecimiento frente a la integración institucional de la gestión de riesgos de seguridad de la información dentro del marco general de gestión del riesgo, dado que, aunque el Manual PLE-PIN-M001 V9 establece lineamientos, procedimientos, formatos y responsabilidades para su administración, no se evidenció implementación homogénea del modelo en todas las dependencias y Alcaldías Locales evaluadas.

Durante la revisión realizada se observó que la Dirección de Tecnologías e Información – DTI participa activamente en actividades de formulación, monitoreo y seguimiento de riesgos de seguridad de la información; de acuerdo con el rol establecido, sin embargo, no se evidenciaron suficientes soportes documentales asociados a validaciones metodológicas, monitoreo independiente o trazabilidad de seguimiento. Lo que se evidencia como una oportunidad de fortalecimiento frente a las funciones, monitoreo independiente y articulación institucional del modelo de líneas de defensa aplicado a riesgos tecnológicos y de seguridad digital.

En consecuencia, se identifican oportunidades de fortalecimiento frente a la formalización e integración de la gestión de riesgos de seguridad de la información dentro del marco institucional de gestión del riesgo, promoviendo una mayor articulación con:

- la política institucional de riesgos,
- las líneas de defensa,
- el MSPI,
- los instrumentos metodológicos definidos por la Entidad, bajo un enfoque integral orientado a la gestión de riesgos tecnológicos y amenazas emergentes de seguridad digital.

La OCI recomienda fortalecer la cobertura institucional de las matrices de riesgos de seguridad de la información, así como los mecanismos de monitoreo, seguimiento y validación metodológica, garantizando trazabilidad, segregación de funciones y aplicación homogénea del modelo en el Nivel Central y Local.

### 7.2.2.3. Identificación y descripción del riesgo

Para el análisis metodológico de la formulación de riesgos de seguridad de la información, la Oficina de Control Interno seleccionó una muestra de siete (7) riesgos clasificados en niveles extremo, alto y moderado, correspondientes al Nivel Central y Nivel Local.

La revisión se efectuó conforme a los lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7, verificando particularmente:

- claridad en la definición del evento de riesgo;
- identificación de causas, amenazas y vulnerabilidades;
- definición de consecuencias o impactos;
- coherencia metodológica frente a los principios de disponibilidad, integridad y confidencialidad de la información.

A continuación, se presentan los resultados del análisis efectuado.

Tabla 14. Análisis descripción del riesgo

RIESGO FORMULADO	PROCESO	RIESGO INHERENTE	OBSERVACIÓN GUÍA DE RIESGOS
Riesgo 1: Pérdida de la integridad por información imprecisa o inexacta en las operaciones.	Gestión Políciva	Extremo	La formulación identifica el evento asociado a la pérdida de integridad de la información; no obstante, no desarrolla de manera suficiente las causas o vulnerabilidades que podrían originar la materialización del riesgo, ni las consecuencias operacionales, jurídicas o institucionales derivadas de la afectación a la integridad de la información. Conforme a la Guía V7, la formulación debe incorporar claramente causa, evento e impacto
Riesgo 2: Pérdida, dispersión o inaccesibilidad de la información institucional debido a la ausencia de tablas de retención documental, la inexistencia de un repositorio único de gestión documental y la desagregación de datos en múltiples sistemas de información (JACD, ORFEO), lo cual dificulta la trazabilidad, custodia y conservación de los registros.	Gestión Políciva	Extremo	El riesgo presenta adecuada identificación de amenazas, vulnerabilidades y consecuencias asociadas a la pérdida de información institucional, alineándose metodológicamente con los lineamientos de la Guía V7. No obstante, la formulación resulta extensa y puede simplificarse para mejorar su claridad, trazabilidad y monitoreo dentro de la matriz de riesgos.
Riesgo 5: Pérdida en la trazabilidad de las operaciones realizadas en relación con actividades de I.V.C.	Gestión Políciva	Extremo	La formulación presenta un nivel de generalidad que dificulta identificar claramente las causas, amenazas o vulnerabilidades asociadas a la pérdida de trazabilidad de las operaciones de IVC. Así mismo, no se evidencian consecuencias específicas derivadas de la materialización del riesgo, limitando su adecuada valoración y definición de controles.
Riesgo 1: Incumplimiento regulatorio de las leyes del gobierno nacional en materia de seguridad de la información y de las políticas de seguridad y privacidad de la información que atenten contra la disponibilidad, integridad y confidencialidad de la información de la Secretaría Distrital de Gobierno.	Servicio de atención a la ciudadanía	Moderado	El riesgo identifica el incumplimiento normativo asociado a seguridad y privacidad de la información, así como afectaciones sobre los principios de disponibilidad, integridad y confidencialidad; no obstante, la formulación mezcla en una misma estructura causas, evento e impacto, dificultando la diferenciación metodológica requerida por la Guía V7 para su adecuada valoración y tratamiento.
Riesgo 1:	Alcaldía Local de Engativá	Extremo	El riesgo identifica afectaciones relacionadas con continuidad operativa y disponibilidad de la información; sin embargo, las causas asociadas presentan un nivel de

RIESGO FORMULADO	PROCESO	RIESGO INHERENTE	OBSERVACIÓN GUÍA DE RIESGOS
Pérdida de la continuidad de los servicios u operaciones de la entidad por ausencia o demora de la información o de los sistemas para las operaciones.			ambigüedad que dificulta identificar claramente las vulnerabilidades o condiciones tecnológicas que originan el riesgo. La Guía V7 recomienda formular riesgos específicos y trazables que permitan facilitar su monitoreo y tratamiento.
Riesgo 1: Pérdida de la integridad por información imprecisa o inexacta de las operaciones, debido a modificación no autorizada o no deliberada en el proceso de generación, recolección, procesamiento y/o almacenamiento.	Alcaldía Local de San Cristóbal	Moderado	La formulación presenta adecuada estructura metodológica, identificando el evento y las causas asociadas a modificaciones no autorizadas o accidentales de la información. No obstante, puede fortalecerse mediante la incorporación de impactos institucionales, operacionales o reputacionales derivados de afectaciones a la integridad de la información.
Riesgo 3: Fallas en la infraestructura tecnológica o falta de mantenimiento en componentes tecnológicos.	Gerencia TIC	Alto	La formulación describe condiciones asociadas a vulnerabilidades tecnológicas y mantenimiento de infraestructura; sin embargo, no define claramente el evento de riesgo ni las consecuencias institucionales derivadas de posibles fallas en los componentes tecnológicos. Conforme a la Guía V7, la formulación debe describir de manera precisa qué puede ocurrir y cuál sería la afectación sobre la operación institucional y los servicios tecnológicos.

Fuente: Elaboración OCI con la información aportada por DTI

Del análisis realizado sobre la muestra evaluada, se evidenció que las principales oportunidades de fortalecimiento en la formulación de riesgos de seguridad de la información se relacionan con:

- identificación clara de amenazas y vulnerabilidades;
- diferenciación entre causas, evento e impacto;
- incorporación de consecuencias institucionales;
- precisión metodológica en la descripción del riesgo.

Así mismo, se observó que varios riesgos se encuentran orientados principalmente a afectaciones sobre disponibilidad e integridad de la información, particularmente frente a:

- continuidad operativa,
- trazabilidad,
- gestión documental,
- seguridad de los sistemas de información.

No obstante, en algunos casos las formulaciones presentan descripciones generales o extensas que podrían dificultar:

- el monitoreo del riesgo,
- la definición de controles específicos,
- la evaluación de efectividad,

- la adecuada valoración del riesgo residual.

En consecuencia, se recomienda fortalecer metodológicamente la formulación de riesgos de seguridad de la información, promoviendo estructuras más claras, específicas y alineadas con los lineamientos establecidos en la Guía V7 y el Modelo de Seguridad y Privacidad de la Información – MSPI.

La OCI recomienda fortalecer el acompañamiento metodológico y la validación técnica de las matrices de riesgos de seguridad de la información, garantizando homogeneidad en la formulación de riesgos y trazabilidad en su valoración y monitoreo.

#### **7.2.2.4. Diseño y análisis de controles de seguridad de la información**

Como resultado de la revisión efectuada sobre los controles asociados a la muestra de riesgos de seguridad de la información, se evidenció que, en términos generales, estos guardan relación con los riesgos identificados y se orientan principalmente a:

- seguimiento,
- control de accesos,
- respaldo de información,
- capacitación,
- soporte tecnológico.

No obstante, se identifican oportunidades de fortalecimiento frente a la estructuración metodológica de algunos controles, particularmente en aspectos relacionados con:

- definición de responsables,
- periodicidad,
- mecanismos de verificación,
- evidencias de ejecución,
- trazabilidad del monitoreo,  
conforme a los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo V7.

Durante la revisión realizada se observó que algunos controles se encuentran formulados como actividades operativas o acciones generales, sin incorporar de manera suficiente elementos metodológicos asociados a:

- responsables específicos,
- frecuencia de ejecución,
- mecanismos de seguimiento,
- criterios de validación,
- y evidencias documentales.

Así mismo, en algunos casos no se evidenciaron soportes o registros suficientes que permitieran validar la trazabilidad y monitoreo del control formulado.

Adicionalmente, se identificó que algunos controles describen herramientas tecnológicas o actividades administrativas; no obstante, no definen claramente la acción de control orientada a prevenir, detectar o mitigar el riesgo asociado.

En consecuencia, se identifican oportunidades de fortalecimiento frente a la formulación, formalización y seguimiento de controles de seguridad de la información, particularmente en aspectos relacionados con monitoreo, trazabilidad y evaluación de efectividad.

Tabla 15. Análisis descripción de controles

PROCESO ASOCIADO / RIESGO	CONTROLES FORMULADOS	NATURALEZA DEL CONTROL	OBSERVACIÓN GUÍA DE RIESGOS
Gestión Policiva Riesgo 1  <b><i>Pérdida de la integridad por información imprecisa o inexacta en las operaciones.</i></b>	Seguimiento oportuno a los casos HOLA y soporte técnico por parte del área técnica funcional de la DGP a las inspecciones de policía en relación con el instructivo GET-IVC-IN014.	Preventivo	El control describe una actividad operativa; sin embargo, no define claramente responsable puntual, evidencia generada, periodicidad de ejecución ni mecanismo de verificación, elementos requeridos por la guía para una adecuada estructuración del control. Adicionalmente, no se evidencian soportes ni seguimiento documentado.
	Aplicación de estrategia de capacitación, retroalimentación y soporte técnico en SIACTUA por parte de la DGP.	Preventivo	El control se encuentra formulado de manera general y no especifica criterios de medición, frecuencia, responsables ni evidencias que permitan validar su ejecución y efectividad, conforme a los lineamientos metodológicos de la guía.
	Solicitudes de validación de usuarios activos en la herramienta SIACTUA a los Fondos de Desarrollo Local realizada por parte de DGP.	Detectivo/Correctivo	El control guarda relación con la gestión de accesos; no obstante, requiere definir formalmente cómo se realiza la validación, quién la aprueba, con qué periodicidad y cuáles son las evidencias de control generadas.
Gestión Policiva Riesgo 2  <b><i>Pérdida, dispersión o inaccesibilidad de la información institucional debido a la ausencia de tablas de retención documental, la inexistencia de un repositorio único de gestión documental y la desagregación de datos en múltiples sistemas de información (JACD, ORFEO), lo cual dificulta la trazabilidad, custodia y conservación de los registros</i></b>	Implementación de Base de datos SharePoint "Registro de parques".	Preventivo	El control incorpora herramientas orientadas al fortalecimiento de la trazabilidad y almacenamiento de información; sin embargo, requiere definir responsables, periodicidad de actualización y mecanismos de seguimiento que permitan evaluar su operación y efectividad.
	Actualización sistemática del listado de parques registrados publicado en página web y micrositio.	Preventivo	El control describe actividades de actualización de información institucional; no obstante, requiere fortalecer elementos asociados a frecuencia, validación, monitoreo y evidencias documentales.
	Base de datos de resoluciones emitidas JACD en OneDrive con accesos determinados.	Preventivo	El control incorpora restricciones de acceso; no obstante, la guía establece que deben documentarse los mecanismos de administración de permisos, responsables y monitoreo de accesos para garantizar la efectividad del control.
	Carpeta OneDrive de delegados con accesos específicos y respaldo en ORFEO.	Preventivo	El control incorpora medidas relacionadas con restricción de accesos y almacenamiento de información; sin embargo, no se evidencian mecanismos documentados de revisión periódica.

PROCESO ASOCIADO / RIESGO	CONTROLES FORMULADOS	NATURALEZA DEL CONTROL	OBSERVACIÓN GUÍA DE RIESGOS
			administración de permisos y monitoreo de accesos
	Control de gestión de delegados a través de formulario online con usuarios específicos.	Preventivo	El control no describe claramente el objetivo del control, responsables, periodicidad ni evidencias generadas, por lo que dificulta verificar su aplicación y efectividad.
	Base de datos alternativa en OneDrive de control de delegaciones y stock de sellos de seguridad.	Detectivo/Correctivo	El control se orienta a mantener respaldo de información; sin embargo, requiere definir actividades de monitoreo, actualización y responsables del control para alinearse con la metodología de la guía.
<p>Gestión Políciva Riesgo 5</p> <p><b><i>Pérdida en la trazabilidad de las operaciones realizadas en relación con actividades de I.V.C</i></b></p>	Diseño e implementación de herramienta SharePoint donde repose la información de la Dirección por cada vigencia.	Preventivo	El control describe una herramienta tecnológica orientada al almacenamiento de información; no obstante, requiere formalizar procedimientos asociados a administración, actualización, monitoreo y validación del control.
	Establecimiento de un archivo único de control de acceso a SharePoint con listado de personas con acceso.	Preventivo	El control incorpora medidas de restricción de acceso; sin embargo, no se evidencia definición de revisión periódica de permisos, trazabilidad de accesos ni soportes de seguimiento.
	Consolidación de la información en un reporte cualitativo mensual en carpeta individual.	Preventivo	El control establece una actividad de consolidación documental, pero requiere definir responsables, mecanismos de validación y evidencias que permitan verificar el cumplimiento del control.
	Traslado de información soporte tipo copia de seguridad en carpeta única relacionada con IVC.	Preventivo	El control corresponde a una actividad de respaldo de información; no obstante, no define periodicidad, responsables, pruebas de restauración ni evidencias de ejecución del respaldo.
	Establecimiento de un tablero de control de actividades y operativos IVC para control de metas.	Detectivo/Correctivo	El control se enfoca en seguimiento operativo; sin embargo, la guía requiere establecer claramente criterios de monitoreo, responsables, frecuencia y evidencias generadas.
<p>Servicio de atención a la ciudadanía – Riesgo 1</p> <p><b><i>Incumplimiento regulatorio de las leyes del gobierno nacional en materia de seguridad de la información y de las políticas de seguridad y privacidad de la información que atenten contra la disponibilidad, integridad y confidencialidad de la</i></b></p>	Generar un reporte trimestral de los registros y cancelaciones de usuarios vinculados al proceso SAC, garantizando la adecuada gestión de los derechos de acceso a los sistemas institucionales, como correo electrónico, casos HOLA, ORFEO y OneDrive	Preventivo	El control presenta una estructura alineada con la guía, dado que define la actividad específica, periodicidad y el propósito del control relacionado con la gestión de accesos. No obstante, requiere precisar el responsable de su ejecución, los criterios de validación del reporte y las evidencias que soportarán el monitoreo.
		Preventivo	El control establece periodicidad y mecanismo de registro; sin embargo, la

PROCESO ASOCIADO / RIESGO	CONTROLES FORMULADOS	NATURALEZA DEL CONTROL	OBSERVACIÓN GUÍA DE RIESGOS
<i>información de la secretaría distrital de gobierno</i>	Complementos Llevar un control trimestral de registro de los casos HOLA, donde se solicitan los mantenimientos correspondientes o por posibles novedades del servicio que ameriten el soporte técnico y tecnológico.		formulación se orienta más a una actividad operativa que a un control preventivo o detectivo claramente definido. Se recomienda especificar responsables, criterios de revisión, mecanismos de seguimiento y evidencias documentales que permitan verificar su efectividad frente al riesgo identificado.
	Llevar un control trimestral de registro de los correos y/o casos HOLA donde se solicitan las necesidades de uso de los recursos y capacidad futura de procesamiento y almacenamiento, para asegurar el desempeño requerido del sistema.	Preventivo	El control se encuentra relacionado con la gestión de capacidad y disponibilidad de los sistemas, alineándose con buenas prácticas de seguridad de la información. No obstante, requiere fortalecer su estructura metodológica definiendo claramente responsables, acciones derivadas del monitoreo y evidencias que permitan validar su efectividad.
	Generar un reporte trimestral del Sharepoint que permita validar el listado de usuarios que tienen acceso a los archivos e información dispuesta en esta herramienta.	Preventivo	El control guarda coherencia con la gestión de accesos y trazabilidad de la información, incluyendo periodicidad y mecanismo de validación. Sin embargo, la guía recomienda incorporar responsables específicos, criterios de revisión de permisos y soportes de seguimiento que evidencien la aplicación efectiva del control.
	Consolidar por cada trimestre y mantener actualizado el listado del personal vinculado al proceso de Servicio de Atención a la Ciudadanía que ha suscrito el Acuerdo de Confidencialidad.	Preventivo	El control contribuye al fortalecimiento de la confidencialidad de la información y presenta una periodicidad definida; no obstante, requiere complementar elementos metodológicos como responsable del control, mecanismos de validación, trazabilidad documental y seguimiento al cumplimiento de la suscripción de los acuerdos de confidencialidad.
	Identificar los activos asociados a la información y a las instalaciones de procesamiento de información, elaborando y manteniendo actualizado el inventario correspondiente. Asimismo, garantizar que el recurso humano vinculado al proceso SAC reciba la pedagogía o capacitación en Seguridad de la Información, una vez por semestre.	Preventivo	El control incorpora medidas relacionadas con gestión de activos y fortalecimiento de capacidades en seguridad de la información, alineadas con los lineamientos de la guía. Sin embargo, se observa que en una misma formulación se integran dos controles diferentes (inventario de activos y capacitación), lo que puede dificultar su monitoreo y evaluación independiente. Se recomienda separarlos y definir para cada uno responsables, periodicidad, mecanismos de seguimiento y evidencias de ejecución.
Alcaldía Local Engativá – Riesgo 1	Control y custodia de la llave del Data Center.	Preventivo	El control no define responsables; no se evidencian mecanismos de registro de

PROCESO ASOCIADO / RIESGO	CONTROLES FORMULADOS	NATURALEZA DEL CONTROL	OBSERVACIÓN GUÍA DE RIESGOS
<i>Pérdida de la continuidad de los servicios u operaciones de la entidad por ausencia o demora de la Información o de los sistemas para las operaciones.</i>			ingresos, monitoreo ni soportes que permitan validar la trazabilidad del control.
	Rack de comunicaciones y refrigeración – contratación proyectada 2026.	Preventivo	La formulación corresponde a una necesidad o acción proyectada y no a un control implementado. Conforme a la guía, el control debe encontrarse definido, formalizado y operativo.
	Equipos activos, segmentación de redes y autenticación de usuarios.	Preventivo	El control describe medidas generales de seguridad tecnológica, pero no define responsables, procedimientos, periodicidad ni mecanismos de monitoreo y seguimiento.
	Redes WiFi, cambio de contraseñas.	Detectivo/Correctivo	El control requiere precisar frecuencia de cambio, responsables, criterios de seguridad y evidencias de ejecución para garantizar trazabilidad y efectividad.
	Equipos activos – mantenimientos preventivos proyectados 2026.	Detectivo/Correctivo	El control corresponde a una actividad proyectada y no evidencia implementación ni seguimiento efectivo conforme a los lineamientos de la guía.
Alcaldía Local San Cristóbal - Riesgo 1  <i>Pérdida de la integridad por información imprecisa o inexacta de las operaciones, debido a modificación no autorizada o no deliberada en el proceso de generación, recolección, procesamiento y/o almacenamiento.</i>	Establecimiento de permisos para los usuarios acorde a su área y las funciones de esta.	Preventivo	El control guarda relación con gestión de accesos; sin embargo, requiere establecer procedimientos de aprobación, revisión periódica y evidencia de seguimiento a permisos asignados.
	Capacitación continua del personal, considerando responsabilidades, errores comunes y actualizaciones, como medio para mitigar el riesgo.	Preventivo	El control está orientado a fortalecimiento de capacidades; no obstante, debe definir periodicidad, responsables, criterios de evaluación y soportes de asistencia o ejecución.
Gerencia TIC – Riesgo 3  <i>Fallas en la infraestructura tecnológica o falta de mantenimiento en componentes tecnológicos</i>	Desarrollo, evaluación, implementación y seguimiento mensual al plan de trabajo sobre infraestructura tecnológica y mantenimiento.	Detectivo/Correctivo	El control presenta una estructura más completa al incluir seguimiento y generación de reportes; sin embargo, requiere formalizar indicadores, evidencias de monitoreo y responsables específicos del control para medir su efectividad.

Fuente: Elaboración OCI con la información aportada por DTI

Como resultado de la revisión efectuada sobre la muestra seleccionada, se evidenció que varios controles asociados a riesgos de seguridad de la información se encuentran orientados principalmente a:

- gestión de accesos,
- respaldo de información,
- monitoreo operativo,
- capacitación,
- soporte tecnológico,
- trazabilidad documental.

No obstante, se identifican oportunidades de fortalecimiento relacionadas con:

- formalización metodológica de controles,
- definición de responsables,
- periodicidad de ejecución,
- mecanismos de seguimiento,
- evidencias documentales,
- indicadores de efectividad,
- trazabilidad del monitoreo.

Así mismo, se observó que en algunos casos los controles se encuentran formulados como actividades operativas, herramientas tecnológicas o acciones proyectadas, sin diferenciar claramente la acción específica de control orientada a prevenir, detectar o mitigar el riesgo identificado.

En consecuencia, se recomienda fortalecer metodológicamente la estructuración, formalización y monitoreo de controles de seguridad de la información, alineándolos con los lineamientos establecidos en la Guía V7 y el Modelo de Seguridad y Privacidad de la Información – MSPI.

La OCI recomienda fortalecer los mecanismos de monitoreo y evaluación de efectividad de controles tecnológicos y de seguridad digital, garantizando trazabilidad, segregación de funciones y soportes documentales que permitan validar su adecuada implementación y operación.

#### **7.2.2.5. Valoración Riesgo Inherente / Riesgo Residual**

A continuación, se presentan los resultados del análisis comparativo entre la valoración del riesgo inherente y el riesgo residual de los riesgos de seguridad de la información identificados por la Entidad, desagregados por proceso y Nivel Local.

El análisis se efectuó considerando:

- nivel de criticidad del riesgo,
- opciones de manejo,
- controles implementados,
- comportamiento del riesgo residual posterior a la aplicación de controles, conforme a los lineamientos definidos en la Guía para la Gestión Integral del Riesgo V7 y el Modelo de Seguridad y Privacidad de la Información – MSPI.

Tabla 16. Riesgo inherente Vrs. Riesgo residual

TIPO DE PROCESO	PROCESO	CANT. DE RIESGOS	CALIFICACIÓN RIESGO INHERENTE				OPCIONES DE MANEJO (Opciones de tratamiento del riesgo)			CANT. DE CONTROLES	CALIFICACIÓN RIESGO RESIDUAL			
			EXT	ALT	MOD	BAJ	RED	ASU	EVI		EXT	ALT	MOD	BAJ
ESTRATÉGICO	Oficina Asesora de Planeación	5	0	2	2	1	4	1	0	8	0	0	4	1
MISIONAL	DGP (Dirección para la Gestión Policiva)	5	3	2	0	0	2	0	3	20	1	0	1	3
	Dirección de la Gestión para el Desarrollo Local	3	0	1	0	2	1	2	0	5	0	0	0	1
	Protección de los derechos étnicos	1	0	0	0	1	0	1	0	3	0	0	0	0
	Convivencia y Dialogo Social	3	0	1	2	0	3	0	0	7	0	0	0	3
	Subsecretaría de Gestión Local	2	0	0	2	0	2	0	0	7	0	0	0	2
	Derechos humanos	1	0	1	0	0	1	0	0	4	0	0	0	0
APOYO	OCDI (Oficina de Control Disciplinario Interno)	1	0	1	0	0	1	0	0	2	0	0	1	0
	Dirección de Contratación	2	0	1	1	0	2	0	0	6	0	0	1	1
	Dirección Gestión Jurídica	3	0	0	0	3	0	3	0	14	0	0	0	3
	SGI (Subsecretaría de Gestión Institucional)	6	0	2	1	3	3	3	0	6	0	0	1	5
EVALUACIÓN Y MEJORA	Oficina de control interno	1	0	0	1	0	1	0	0	2	0	0	1	0
TRANSVERSAL	Servicio de atención a la ciudadanía	1	0	0	1	0	1	0	0	6	0	0	0	1

TIPO DE PROCESO	PROCESO	CANT. DE RIESGOS	CALIFICACIÓN RIESGO INHERENTE				OPCIONES DE MANEJO (Opciones de tratamiento del riesgo)			CANT. DE CONTROLES	CALIFICACIÓN RIESGO RESIDUAL			
			EXT	ALT	MOD	BAJ	RED	ASU	EVI		EXT	ALT	MOD	BAJ
<b>NIVEL LOCAL</b>														
BARRIOS UNIDOS		14	0	6	8	0	14	0	0	43	0	0	3	11
SAN CRISTOBAL		7	0	2	3	2	5	2	0	16	0	0	5	2
ENGATIVÁ		5	1	0	4	0	4	0	1	11	0	1	3	1
PUENTE ARANDA		5	0	0	3	2	3	2	0	15	0	0	1	4
TEUSAQUILLO		3	0	3	0	0	3	0	0	5	0	0	1	2
<b>18 mapas de riesgos</b>		<b>68</b>	<b>4</b>	<b>22</b>	<b>28</b>	<b>14</b>	<b>50</b>	<b>14</b>	<b>4</b>	<b>180</b>	<b>1</b>	<b>1</b>	<b>22</b>	<b>40</b>

Fuente: Elaboración propia OCI con base en reporte de la OAP

Del total de 68 riesgos evaluados en su valoración inherente:

- 4 riesgos (5,8 %) se clasifican en zona extrema;
- 22 riesgos (32,4 %) en zona alta;
- 28 riesgos (41,1 %) en zona moderada;
- y 14 riesgos (20,5 %) en zona baja.

Lo anterior evidencia una mayor concentración de riesgos en niveles moderados y altos, particularmente asociados a procesos misionales y del Nivel Local, relacionados con disponibilidad, integridad, continuidad operativa y gestión de accesos a la información institucional.

El análisis comparativo entre riesgo inherente y residual evidenció que cuatro (4) riesgos no cuentan con valoración residual registrada, correspondientes a los procesos:

- Dirección de la Gestión para el Desarrollo Local;
- y Protección de los Derechos Étnicos y Derechos Humanos.

Lo anterior limita la trazabilidad metodológica y el análisis del comportamiento residual del riesgo posterior a la aplicación de controles, dificultando el seguimiento y evaluación de las medidas de tratamiento implementadas.

Así mismo, se observó que:

- uno (1) de los riesgos clasificados inicialmente en zona extrema mantiene la misma valoración residual, asociado a la Dirección para la Gestión Policial;

- mientras que los riesgos clasificados inicialmente en zona alta registran disminución en su valoración residual hacia categorías moderadas o bajas, conforme a la metodología de valoración aplicada en las matrices institucionales.

No obstante, aunque se observa una reducción general en la valoración residual de varios riesgos, ello no implica por sí mismo plena efectividad de los controles implementados, dado que dicha evaluación requiere considerar adicionalmente aspectos relacionados con:

- operación efectiva del control,
- monitoreo periódico,
- trazabilidad documental,
- gestión del riesgo residual,
- y seguimiento sobre incidentes materializados o desviaciones identificadas.

Adicionalmente, se evidenció una mayor concentración de opciones de tratamiento orientadas a la reducción del riesgo, particularmente mediante controles preventivos asociados a:

- gestión de accesos,
- respaldo de información,
- monitoreo tecnológico,
- capacitación,
- y continuidad operativa.

No obstante, se identifican oportunidades de fortalecimiento frente a la evaluación de efectividad de dichos controles y al seguimiento del riesgo residual, especialmente en riesgos asociados a disponibilidad, integridad y trazabilidad de la información institucional.

En términos generales, se evidencian avances en la implementación de mecanismos de tratamiento orientados a la mitigación de riesgos de seguridad de la información; sin embargo, se identifican oportunidades de fortalecimiento relacionadas con:

- formalización de valoraciones residuales,
- seguimiento metodológico,
- evaluación de efectividad de controles,
- trazabilidad del monitoreo,
- y consolidación de indicadores asociados al comportamiento del riesgo residual.

Así mismo, resulta necesario fortalecer el análisis periódico de riesgos tecnológicos y de seguridad digital, promoviendo mecanismos de seguimiento continuo y mejora permanente conforme a los lineamientos establecidos en la Guía V7 y el Modelo de Seguridad y Privacidad de la Información – MSPI.

#### **7.2.2.6. Resultados del Monitoreo**

El análisis realizado evidenció que, aunque la entidad cuenta con lineamientos y matrices para la gestión de riesgos de Seguridad de la Información, el Manual de Gestión del Riesgo aborda de manera general la identificación de activos de información, sin profundizar en aspectos metodológicos relacionados con identificación de riesgos específicos, controles, tratamientos, monitoreo y responsables del seguimiento.

Para la verificación se tomó una muestra de siete (7) riesgos de un total de sesenta y ocho (68), equivalente al 10,29 % del universo evaluado, priorizando riesgos clasificados en niveles extremo, alto y moderado de los procesos de Gestión Policiva, Gerencia TIC, Servicio a la Ciudadanía y Alcaldías Locales de Engativá y San Cristóbal.

Durante la revisión de las dieciocho (18) matrices aportadas por la Dirección de Tecnologías e Información – DTI, no se evidenció reporte documentado de riesgos materializados de seguridad de la información dentro de la información suministrada para análisis.

No obstante, se observó que la mayoría de las matrices se encuentran en etapas iniciales de implementación y construcción metodológica, con vigencias comprendidas entre 2025 y 2026.

Así mismo, aunque las matrices incorporan elementos asociados a:

- riesgos,
- controles,
- acciones preventivas,
- responsables,
- evidencias esperadas,
- y planes de tratamiento,

no se evidenciaron soportes, registros o trazabilidad suficientes que permitieran validar la ejecución efectiva de los controles y actividades de monitoreo definidas.

Así mismo, se identificó que los campos asociados a seguimiento y monitoreo, tales como:

- materialización del riesgo,
- reporte de incidentes,
- análisis de causas,
- seguimiento de controles,
- y evidencias de ejecución,

se encuentran, en varios casos, sin diligenciar dentro de las matrices revisadas.

Lo anterior limita la trazabilidad del monitoreo y dificulta realizar evaluación objetiva sobre:

- operación de controles,
- seguimiento del riesgo residual,
- efectividad de medidas implementadas,
- y madurez del proceso de gestión de riesgos de seguridad de la información, conforme a los lineamientos establecidos en la Guía V7 y el MSPI.

En términos generales, se evidencian avances en la formulación e implementación inicial de matrices de riesgos de seguridad de la información; no obstante, se identifican oportunidades de fortalecimiento relacionadas con:

- formalización documental,
- trazabilidad del monitoreo,
- reporte de incidentes,
- seguimiento del riesgo residual,
- documentación de evidencias,

- y evaluación de efectividad de controles tecnológicos.

Así mismo, se observa que el modelo institucional de gestión de riesgos de seguridad de la información se encuentra en una etapa de madurez en desarrollo, particularmente frente a componentes asociados a monitoreo continuo, seguimiento documentado y consolidación de mecanismos de control y trazabilidad.

La OCI recomienda fortalecer los mecanismos de monitoreo, seguimiento y documentación de riesgos de seguridad de la información, garantizando trazabilidad sobre incidentes, operación de controles y evaluación periódica de la efectividad de las medidas implementadas

### **7.2.3. Riesgos de Corrupción - Gestión de riesgos para la integridad pública (SIGRIP)**

La Guía para la Gestión Integral del Riesgo – Versión 7 del DAFP incorpora el enfoque de Riesgos para la Integridad Pública (SIGRIP), propuesto por la Secretaría de Transparencia de la Presidencia de la República en el marco de la Ley 2195 de 2022, con el propósito de fortalecer los mecanismos institucionales orientados a la prevención, detección, monitoreo y tratamiento de riesgos que puedan afectar la integridad del servicio público y la confianza institucional.

En Manual de Gestión del Riesgo de la Entidad (Código: PLE-PIN-M001, Versión 09), particularmente en el capítulo 12, se identificó que los lineamientos desarrollados se orientan principalmente a riesgos asociados a posibles actos de soborno y corrupción.

En este sentido, se identifican oportunidades de mejora frente a la consolidación de una metodología integral de gestión de riesgos para la integridad pública, que permita incorporar de manera articulada las diferentes tipologías de riesgo contempladas en la Guía V7, así como aquellas derivadas del contexto institucional, cambios normativos y condiciones del entorno operativo.

Así mismo, se recomienda fortalecer la articulación de dicho enfoque con las instancias institucionales de gobernanza y líneas de defensa, garantizando alineación con los lineamientos del DAFP y demás disposiciones técnicas aplicables

#### **7.2.3.1. Herramientas para la gestión del riesgo**

Para la gestión de riesgos de corrupción e integridad pública, la Entidad cuenta con herramientas metodológicas y documentales orientadas a la identificación, análisis, monitoreo y seguimiento de riesgos, soportadas principalmente en los siguientes instrumentos institucionales:

- PLE-PIN-M001 Manual de Gestión del Riesgo
- PLE-PIN-P015 Administración y Monitoreo de Riesgos de Gestión y Corrupción
- PLE-PIN-F035 Formato Matriz Monitoreo de Riesgos
- Un (1) mapa con 30 riesgos identificados en los diferentes procesos.

Los riesgos de corrupción se encuentran consolidados en un único mapa institucional; no obstante, durante la revisión realizada no se evidenció segregación metodológica suficiente que permitiera diferenciar claramente aquellos riesgos asociados específicamente al Nivel Central frente a los que presentan alcance en el Nivel Local.

Lo anterior evidencia oportunidades de fortalecimiento frente a la incorporación de enfoques diferenciales y territoriales dentro de la gestión de riesgos de corrupción e integridad pública

**Análisis de Contexto y DOFA:** De acuerdo con la revisión efectuada, no se evidenció incorporación documentada de análisis de contexto y matriz DOFA dentro de los formatos PLE-PIN-F002 aportados para análisis, limitando la identificación de factores internos y externos asociados a riesgos de corrupción e integridad pública.

**Lineamientos de Adopción y Articulación Institucional:** La revisión documental permitió evidenciar que los roles y responsabilidades frente a la gestión de riesgos se encuentran definidos en el marco de las líneas de defensa establecidas en el documento PLE-PIN-M001 Manual de Gestión del Riesgo.

Asimismo, se identificó que la Oficina Asesora de Planeación (OAP) es la responsable de brindar apoyo metodológico en las etapas de creación y modificación de las matrices de riesgos de gestión. En este sentido, los profesionales del Equipo de Riesgos de la OAP realizan el análisis metodológico sobre la formulación efectuada por cada líder de proceso, verificando aspectos relacionados con:

- La coherencia entre la redacción del riesgo y el objetivo del proceso.
- Las causas que permiten la ocurrencia del riesgo.
- La definición de escalas de probabilidad e impacto acordes con la realidad de las actividades evaluadas.
- La definición de controles que incluyan los elementos requeridos: responsable, actividad de control, periodicidad de ejecución y evidencia.

Para el caso de los riesgos de corrupción, la propuesta de actualización y/o modificación de las matrices deberá ser presentada ante el Comité Institucional de Gestión y Desempeño (CIGD) o el Comité Institucional de Coordinación de Control Interno (CICCI), según corresponda, con el fin de garantizar su revisión, validación y articulación institucional.

Asimismo, se evidenció que la Oficina Asesora de Comunicaciones (OAC) realiza la publicación de las matrices de riesgos de corrupción en la página web de la entidad, garantizando la transparencia, consulta y acceso a la información.

**Monitoreo y Seguimiento:** En relación con las actividades de monitoreo y seguimiento, se evidenció que los procesos y Alcaldías Locales deben consolidar información relacionada con la ejecución de controles asociados a riesgos de corrupción, diligenciando el formato PLE-PIN-F035 y cargando las evidencias correspondientes en los repositorios definidos por la Oficina Asesora de Planeación.

Lo anterior evidencia mecanismos institucionales orientados al monitoreo y trazabilidad de la gestión de riesgos de corrupción; no obstante, se identifican oportunidades de fortalecimiento frente a seguimiento metodológico, evaluación de efectividad de controles y monitoreo del riesgo residual

**Presentación de Resultados y Custodia de la Información:** La Oficina Asesora de Planeación consolida y elabora informes relacionados con la gestión de riesgos, los cuales son publicados en la página web de la entidad como mecanismo de transparencia y divulgación institucional. Los resultados obtenidos son presentados en

sesión del Comité Institucional de Coordinación de Control Interno, permitiendo realizar seguimiento institucional a la gestión de riesgos y fortalecer la toma de decisiones frente a los riesgos identificados.

**Materialización de riesgos:** En las políticas de operación establecidas en el procedimiento PLE-PIN-P015 Administración y monitoreo de riesgos de gestión y corrupción, se dispone que es responsabilidad de cada líder de proceso y/o alcalde local formular los respectivos planes de mejoramiento cuando se evidencie la materialización de riesgos.

Asimismo, para los casos relacionados con la materialización de riesgos de corrupción, el procedimiento establece la obligación de reportar oportunamente la situación ante los entes de control competentes y la Fiscalía, según corresponda, con el fin de garantizar la adopción de las acciones administrativas, disciplinarias, fiscales o penales a que haya lugar.

En términos generales, se evidencian avances institucionales en la incorporación de herramientas para la gestión de riesgos de corrupción; no obstante, se identifican oportunidades de fortalecimiento frente a la consolidación integral del enfoque SIGRIP, particularmente en aspectos relacionados con:

- incorporación de nuevas tipologías de riesgos para la integridad pública;
- análisis de contexto;
- enfoque diferencial territorial;
- monitoreo del riesgo residual;
- y evaluación de efectividad de controles.

Adicionalmente, resulta pertinente considerar las particularidades funcionales y operativas de la estructura institucional de la Secretaría Distrital de Gobierno, especialmente frente al alcance territorial de las Alcaldías Locales y la administración de los Fondos de Desarrollo Local – FDL.

En este contexto, la gestión de riesgos para la integridad pública y riesgos de corrupción requiere incorporar un enfoque diferencial para el Nivel Local, considerando que los Fondos de Desarrollo Local administran recursos públicos superiores a los dos billones de pesos, asociados principalmente a procesos de contratación, ejecución presupuestal, supervisión contractual, inversión local, participación ciudadana y gestión territorial.

Lo anterior implica mayores niveles de exposición frente a riesgos asociados a integridad pública, corrupción, conflictos de interés, gestión contractual, direccionamiento indebido, debilidades en supervisión, riesgos fiscales y afectaciones reputacionales, por lo que se hace necesario que la Política Integral de Gestión del Riesgo contemple de manera expresa lineamientos metodológicos, mecanismos de monitoreo y estrategias de tratamiento diferenciadas para el Nivel Local.

Así mismo, se identifican oportunidades de fortalecimiento frente a:

- segregación y trazabilidad de riesgos entre Nivel Central y Nivel Local;
- incorporación de riesgos asociados a la gestión de los Fondos de Desarrollo Local por parte de los Alcaldes Locales;
- fortalecimiento de controles sobre procesos de contratación e inversión territorial;
- y consolidación de mecanismos de monitoreo diferencial conforme al contexto operativo y presupuestal de las Alcaldías Locales.

En consecuencia, se recomienda fortalecer el enfoque territorial y diferencial de la Política Integral de Gestión del Riesgo, garantizando que la gestión de riesgos para la integridad pública y corrupción incorpore las particularidades administrativas, operativas, presupuestales y funcionales propias del esquema de gobernanza local de la Secretaría Distrital de Gobierno.

### 7.2.3.2. Caracterización riesgos de corrupción

La entidad cuenta con treinta (30) riesgos de corrupción distribuidos en los cinco tipos de procesos institucionales. La mayor concentración se presenta en los procesos de apoyo, con diez (10) riesgos identificados, seguidos de los procesos estratégicos con ocho (8) y los misionales con seis (6), lo que evidencia una mayor exposición al riesgo en las actividades operativas y de soporte de la entidad.

En la verificación realizada por la Oficina de Control Interno (OCI), se evidenció que el Nivel Local no cuenta con un enfoque diferencial para la gestión de los riesgos de corrupción frente al Nivel Central. Asimismo, en la documentación y en los mapas de riesgos aportados por la Oficina Asesora de Planeación, se identificó un único mapa de riesgos de corrupción, sin que exista claridad sobre cuáles riesgos corresponden específicamente al Nivel Central y cuáles tienen alcance en el Nivel Local.

Tabla 17. Caracterización riesgos de corrupción

TIPO PROCESO	CANT RIESGOS	CANT CONTROLES	TIPOLOGÍA DEL CONTROL		
			Preventivo	Detectivo	Correctivo
ESTRATÉGICO	8	11	9	2	0
MISIONAL	6	8	6	2	0
APOYO	10	12	12	0	0
EVALUACIÓN Y MEJORA	5	6	5	1	0
TRANSVERSAL	1	4	4	0	0
<b>TOTAL</b>	<b>30</b>	<b>41</b>	<b>36</b>	<b>5</b>	<b>0</b>

Fuente: Elaboración propia OCI con base en reporte de la OAP

En cuanto a los controles, se evidencia una predominancia de controles preventivos (36 de 41), lo que representa una orientación positiva hacia la anticipación del riesgo. Sin embargo, la presencia de controles detectivos es limitada (5 en total) y no se registran controles correctivos en ninguno de los procesos.

No obstante, la presencia de controles detectivos es limitada (5 controles) y no se evidencian controles correctivos dentro de las matrices revisadas, situación que evidencia oportunidades de fortalecimiento frente a mecanismos institucionales de respuesta, tratamiento y seguimiento posterior a eventos de riesgo materializados.

### 7.2.3.3. Identificación y descripción del riesgo

La Oficina de Control Interno (OCI) realizó revisión metodológica sobre una muestra equivalente al 23 % de los riesgos de corrupción identificados por la Entidad, correspondiente a siete (7) riesgos clasificados en niveles extremo y alto.

El análisis se efectuó conforme a los lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7, verificando particularmente:

- identificación del impacto;
- definición de causas inmediatas y causas raíz;
- coherencia metodológica;
- y claridad conceptual en la formulación del riesgo

En la verificación realizada por la Oficina de Control Interno (OCI), se evidenció que el Nivel Local no cuenta con un enfoque diferencial claramente definido para la gestión de riesgos de corrupción e integridad pública frente al Nivel Central.

Así mismo, en la documentación y matrices aportadas por la Oficina Asesora de Planeación se identificó un único mapa institucional de riesgos de corrupción, sin segregación metodológica suficiente que permita diferenciar claramente:

- los riesgos asociados al Nivel Central;
- los riesgos con alcance en las Alcaldías Locales;
- y aquellos relacionados con la administración de los Fondos de Desarrollo Local – FDL

Lo anterior evidencia una mayor concentración de riesgos asociados a procesos administrativos, de soporte y estratégicos, particularmente en actividades relacionadas con contratación, gestión documental, tecnologías de la información, gestión disciplinaria y manejo de información institucional.

La guía establece que la descripción del riesgo debe contener como elementos mínimos: impacto, causa inmediata y causa raíz. Con base en ello, la OCI identificó los siguientes aspectos relevantes:

Tabla 18. Análisis descripción del riesgo

RIESGO FORMULADO	PROCESO	RIESGO INHERENTE	OBSERVACIÓN OCI
R3. Posibilidad de afectación reputacional por omisión o inoportuna divulgación / publicación de información sobre la gestión contractual en las plataformas de contratación pública, limitando el conocimiento a la ciudadanía por beneficiar a un particular.	Comunicación estratégica	EXTREMO	Cumple con la estructura definida en cuanto a descripción del impacto, causa inmediata y causa raíz.
R5. Posibilidad de afectación reputacional por proferir decisiones disciplinarias contrarias a derecho en beneficio del sujeto procesal o de un interés particular	Control Disciplinario	EXTREMO	Aunque el riesgo incorpora el impacto reputacional asociado a decisiones disciplinarias contrarias a derecho, no se evidencian con suficiente precisión las causas inmediatas y causas raíz que podrían generar la materialización del riesgo.
R13. Probabilidad de afectación reputacional por pérdida, manipulación o alteración de información en repositorios datos institucionales en beneficio de un tercero.	Gerencia TIC	EXTREMO	El riesgo identifica afectaciones reputacionales derivadas de manipulación o alteración de información; no obstante, requiere fortalecer la definición de causas y vulnerabilidades asociadas a la materialización del riesgo
R22. Posibilidad de afectación reputacional por inadecuado uso de prendas y elementos institucionales en beneficio propio o de un tercero para acceder a eventos públicos o privados de complejidad alta en el SUGA y partidos de fútbol acompañados por el programa de goles en paz.	Convivencia y Diálogo Social	EXTREMO	Cumple con la estructura definida en cuanto a descripción del impacto, causa inmediata y causa raíz.
R23. Orientar con calidad y oportunidad a todos los ciudadanos que acudan a la Secretaría Distrital de Gobierno. Así mismo, atender las peticiones, quejas, reclamos, sugerencias, consultas, denuncias por actos de corrupción, felicitaciones, solicitud de acceso a la información y copias en el marco de los trámites y servicios de la entidad, a través de sus canales presencial, telefónico, virtual y redes sociales, reportando periódicamente la percepción de los ciudadanos en relación con la calidad del servicio prestado, lo anterior, con el fin de garantizar sus derechos y brindar una adecuada atención.	Servicio a la ciudadanía	EXTREMO	La formulación presentada no corresponde metodológicamente a un riesgo de corrupción, sino a una descripción funcional y operativa asociada a la atención a la ciudadanía. No se identifica de manera clara el evento de riesgo, las causas ni el posible beneficio indebido asociado a un acto de corrupción, conforme a los lineamientos establecidos en la Guía V7
R2. Posibilidad de afectación reputacional por omisión o inoportuna divulgación/publicación de información sobre la gestión contractual en las plataformas de contratación pública, limitando el conocimiento a la ciudadanía por beneficiar a un particular	Gestión Corporativa Institucional	ALTO	Cumple con la estructura definida en cuanto a descripción del impacto, causa inmediata y causa raíz.
R8. Posibilidad de afectación reputacional por la pérdida, manipulación o alteración intencional de la información y de los expedientes físicos de los procesos, para beneficio propio o de particulares.	Gestión Patrimonio Documental	ALTO	Cumple con la estructura definida en cuanto a descripción del impacto, causa inmediata y causa raíz.

Fuente: Elaboración propia OCI con base en reporte de la OAP

En cuanto a los controles asociados a riesgos de corrupción, se identificó predominio de controles preventivos (36 de 41), orientados principalmente a actividades de validación, revisión documental, monitoreo y seguimiento previo.

No obstante, la presencia de controles detectivos es limitada (5 controles) y no se evidencian controles correctivos dentro de las matrices revisadas, situación que evidencia oportunidades de fortalecimiento frente a mecanismos institucionales de respuesta, tratamiento y seguimiento posterior a eventos de riesgo materializados

En términos generales, los riesgos evaluados evidencian avances metodológicos frente a la incorporación de estructuras asociadas a impacto reputacional y posibles beneficios indebidos derivados de actuaciones contrarias a la integridad pública.

No obstante, durante la revisión realizada se identificaron oportunidades de fortalecimiento relacionadas con:

- definición de causas inmediatas y causas raíz;
- diferenciación entre riesgos, objetivos y funciones operativas;
- precisión conceptual en la formulación;

En consecuencia, se recomienda fortalecer el acompañamiento metodológico adelantado por la segunda línea de defensa, promoviendo formulaciones más claras, específicas y trazables, especialmente frente a riesgos asociados a:

- contratación pública;
- gestión documental;
- tecnologías de la información;
- supervisión contractual;
- y gestión territorial de los Fondos de Desarrollo Local.

Así mismo, resulta necesario incorporar un enfoque diferencial para el Nivel Local dentro de la gestión de riesgos de corrupción e integridad pública, considerando las particularidades operativas, administrativas y presupuestales de las Alcaldías Locales y los Fondos de Desarrollo Local.

#### **7.2.3.4. Diseño y Análisis de Controles**

Dando continuidad al análisis de los 7 riesgos tomados como muestra para la verificación, se realizó seguimiento a los controles de acuerdo con los lineamientos dados por la “*Guía del Dap V7*”, iniciando con la concepción formal del control el cual debe contemplar tres (3) características para la redacción. “*a) responsable de ejecutar el control, b) acción y c) complemento*”, este último debe aludir la “*periodicidad, como se realiza la actividad del control, que pasa con las observaciones o desviaciones y la evidencia de ejecución del control*” y el manual de gestión del riesgo adoptado por la entidad.

Como resultado de la verificación y análisis de la muestra, se evidenció que, en X de los X controles evaluados no se incorporan adecuadamente los aspectos de periodicidad y desviaciones en su estructura de redacción, tal como se detalla a continuación:

PROCESO ASOCIADO / RIESGO	CONTROLES FORMULADOS	NATURALEZA DEL CONTROL	OBSERVACIÓN GUÍA DE RIESGOS
R3. Posibilidad de afectación reputacional por omisión o inoportuna divulgación / publicación de información sobre la gestión contractual en las plataformas de contratación pública, limitando el conocimiento a la ciudadanía por beneficiar a un particular.	<p>Al inicio de cada vigencia el jefe(a) de la Oficina Asesora de Comunicaciones envía el formato CES-F002 "Formato Planeador de necesidades de comunicación" para diligenciamiento de los directivos de las diferentes dependencias de la SDG, quienes deben remitirlo diligenciado con la programación de las comunicaciones para todo el año, como evidencia de la ejecución de este control quedará el formato CES -F002 y el correo electrónico o memorando enviado.</p> <p>Cada vez que se realice una solicitud a la Oficina Asesora de Comunicaciones el/la jefe (a) de la Oficina Asesora de Comunicaciones garantizará que solo se tramitarán los servicios de comunicaciones que lleguen debidamente diligenciados y firmados por el directivo de la dependencia solicitante a través del formato CES-F001 "Formato de Solicitud de Servicios de Comunicaciones". Como evidencia de ejecución del control queda el formato CES-F001.</p>	Preventivo	<p>Cumple con la estructura definida en cuanto a responsable y atributos informativos.</p> <p>Nota: Para la redacción de la acción se deben utilizar verbos como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar</p>
R5. Posibilidad de afectación reputacional por proferir decisiones disciplinarias contrarias a derecho en beneficio del sujeto procesal o de un interés particular	<p>El Auditor designado por el jefe de la Oficina de Asuntos Disciplinarios cada vez que reciba un proyecto de decisión interlocutoria por parte de los profesionales del equipo de la Oficina de Asuntos Disciplinarios verifica que la decisión este ajustada a la ley (constitución, leyes, normas, convenios internacionales) a través del cotejo normativo sobre el tema a tratar. Como evidencia de la ejecución de control queda la base de datos control de decisiones del despacho, donde se relacionan las observaciones de cada uno de los expedientes.</p> <p>En caso de requerir ajuste en el sentido de la decisión de fondo se remitirá al abogado que proyectó la decisión para que lo adecúe, dejando evidencia en el formato de revisión de decisiones interlocutorias CDS-F001 debidamente diligenciado.</p>	Preventivo	<p>Cumple con la estructura definida en cuanto a responsable, acción y atributos informativos.</p> <p>Nota: Para la redacción de la acción se deben utilizar verbos como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar</p>
R13. Probabilidad de afectación reputacional por pérdida, manipulación o alteración de información en repositorios datos institucionales en beneficio de un tercero.	<p>El profesional designado por el (la) director(a) de Tecnologías e Información, responsable de la plataforma de seguridad perimetral realizará el monitoreo permanente a la plataforma tecnológica institucional para identificar las vulnerabilidades ó alertas que se puedan presentar. El seguimiento es a partir de la generación del reporte de cada uno de los elementos utilizados como controles: el Firewall, Web Aplicación Firewall - WAF, Antivirus, accesos a las bases de datos y aplicaciones.</p> <p>En caso de encontrar vulnerabilidades, se aplicará los ajustes de configuración que corresponda según el caso. Como evidencia quedará el reporte mensual con el registro de las vulnerabilidades y los informes de los ajustes aplicados a la configuración. Dicho control se sustenta en el manual GDI-TIC-M004 Manual de Gestión de Seguridad, ítem de seguridad de la información.</p>	Preventivo	<p>Cumple con la estructura definida en cuanto a responsable, acción y atributos informativos.</p> <p>Nota: Para la redacción de la acción se deben utilizar verbos como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar</p>

<p>R22. Posibilidad de afectación reputacional por inadecuado uso de prendas y elementos institucionales en beneficio propio o de un tercero para acceder a eventos públicos o privados de complejidad alta en el SUGA y partidos de fútbol acompañados por el programa de goles en paz.</p>	<p>El director/a o el servidor(a) designado(a), cada vez que un contratista termine su contrato de prestación de servicios o un funcionario se desvincule de la entidad o cambie de área, debe hacer entrega de prendas y material de uso exclusivo de la dirección para garantizar que no se tenga uso diferente a los fines institucionales y registrar la entrega en el formato GDI-GPD-F029 Evidencia de Reunión.</p>	<p>Preventivo</p>	<p>Cumple con la estructura definida en cuanto a responsable, acción y atributos informativos.</p> <p>Nota: Para la redacción de la acción se deben utilizar verbos como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar</p>
<p>R23. Posibilidad de afectación económica y reputacional por beneficiar un grupo de interés con una iniciativa ciudadana sin garantizar la igualdad e imparcialidad</p>	<p>El profesional designado por el/la director(a) o el aliado, cada vez que se vaya a implementar una iniciativa ciudadana verifica el cumplimiento de los criterios de selección de iniciativas, acatando los lineamientos para grupos de particular atención en el marco del proceso, realiza socialización por diferentes medios que permita dar igualdad de acceso a la información, el cual se registra en el formato de evidencia de reunión GDI-GPD-F029, con el fin de dar transparencia e igualdad al proceso.</p> <p>En caso de que se identifique el incumplimiento de lo establecido en la propuesta de la iniciativa luego de surtidas las verificaciones correspondientes y que, sin embargo, esta se haya aprobado beneficiándose sin principio de igualdad y oportunidad; se debe informar al Profesional delegado para iniciativas ciudadanas, de forma que se realice las medidas correspondientes, para que sea en su lugar elegida la iniciativa que por orden continúe en la lista y cumpla los requisitos según modalidad. Como evidencia queda los correos electrónicos y/o registro en el formato evidencia de reunión GDI-GPD-F029.</p>	<p>Preventivo</p>	<p>Cumple con la estructura definida en cuanto a responsable, acción y atributos informativos.</p> <p>Nota: Para la redacción de la acción se deben utilizar verbos como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar</p>

<p>R2. Posibilidad de afectación reputacional por omisión o inoportuna divulgación/publicación de información sobre la gestión contractual en las plataformas de contratación pública, limitando el conocimiento a la ciudadanía por beneficiar a un particular</p>	<p>En el Nivel Central los colaboradores designados por el/la Director/a de Contratación, de manera permanente adelantan la verificación de ausencias documentales de la totalidad de procesos contractuales de la Entidad diligenciando la "Matriz de verificación documental".</p> <p>Cuando se detecta la falta de algún documento de la etapa contractual se envía un memorando trimestral al supervisor del contrato para que subsane la ausencia documental.</p> <p>Como evidencia de la ejecución del control queda la "Matriz de verificación documental" que consolida la revisión de la totalidad de procesos y las comunicaciones (correos electrónicos y memorandos).</p> <p>En el Nivel Local, el/la alcalde (sa) Local, apoyado en la persona que él designe, de manera permanente adelantan la verificación de ausencias documentales de la totalidad de procesos precontractuales y contractuales de la Alcaldía Local. Cuando se detecta la falta de algún documento en la plataforma de Secop II, el abogado responsable del proceso solicita al proveedor (y/o contratista) a través de correo electrónico el cargue del mismo cuando se trate de modalidad de contratación directa.</p> <p>Cuando se detecta la falta de algún documento de la etapa precontractual y contractual en las diferentes modalidades de contratación en la plataforma de Secop II, el abogado responsable del proceso solicita a través de correo electrónico, al profesional designado como apoyo a la supervisión o interventoría del contrato para que subsane la ausencia documental.</p> <p>Como evidencia de la ejecución del control, quedan los correos electrónicos institucionales y las evidencias de verificación de publicación en la plataforma Secop II.</p>	<p>Preventivo</p>	<p>Cumple con la estructura definida en cuanto a responsable, acción y atributos informativos.</p> <p>Nota: Para la redacción de la acción se deben utilizar verbos como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar</p>
---	--	-------------------	---

<p>R8. Posibilidad de afectación reputacional por la pérdida, manipulación o alteración intencional de la información y de los expedientes físicos de los procesos, para beneficio propio o de particulares.</p>	<p>El servidor del archivo central designado por el/la director/a Administrativo/a (para el nivel central) y el servidor designado por el/la alcalde(sa) local (para el nivel local), cada vez que realice el préstamo de un documento o expediente diligenciará el formato GDI-GPD-F018 o GDI-GPD-F021, según corresponda. Al momento de la devolución realizará la revisión de los documentos y/o expedientes para comprobar el estado en que se reciben. Según lo anterior para generar este reporte de los préstamos de documentos, se debe remitir a la Dirección Administrativa por parte del encargado del Archivo Central o Alcaldía Local el formato GDI-GPD-F018 (formato Excel) de manera mensual, en caso de que no se remita este reporte se entenderá que no se realizaron préstamos durante el periodo de reporte.</p> <p>Si en el momento de la devolución del expediente, el encargado del Archivo Central o Alcaldía Local evidencia que no se encuentra completo frente al estado en el que fue prestado, informará al funcionario y al jefe o director de la dependencia a la que le realizó el préstamo a través de una comunicación oficial con copia a la Dirección Administrativa y se dejará registro en el formato GDI-GPD-F023 de acuerdo con los lineamientos establecidos en las instrucciones GDI-GPD-IN012.</p> <p>Como evidencia de la ejecución del control quedan los formatos GDI-GPD-F018, GDI-GPD-F021, GDI-GPD-F023 y las comunicaciones oficiales.</p>	<p>Detectivo</p>	<p>Cumple con la estructura definida en cuanto a responsable, acción y atributos informativos.</p> <p>Nota: Para la redacción de la acción se deben utilizar verbos como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar</p>
--	---	------------------	---

El análisis realizado evidencia que la Entidad presenta avances en el diseño y documentación de controles asociados a los riesgos de corrupción e integridad pública, especialmente en lo relacionado con:

- identificación de responsables;
- definición de actividades de control;
- y establecimiento de evidencias de ejecución.

Así mismo, se observó que los controles evaluados se orientan principalmente a actividades de:

- validación documental;
- seguimiento;
- monitoreo;
- revisión normativa;
- control de accesos;
- y verificación de publicación y trazabilidad de la información institucional.

No obstante, durante la revisión metodológica realizada se identificaron oportunidades de fortalecimiento relacionadas principalmente con la estructura de redacción y formalización de algunos controles. Aunque la mayoría incorpora parcialmente los elementos metodológicos definidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7, persisten oportunidades de mejora frente a:

- incorporación explícita de la periodicidad del control;
- definición clara del tratamiento de desviaciones u observaciones identificadas;

- uso de verbos de control orientados a acciones de verificación, validación, revisión, cotejo, comparación o detección;
- y diferenciación entre actividades operativas y acciones específicas de control.

Así mismo, se evidenció que algunos controles presentan formulaciones extensas y complejas, incorporando múltiples actividades dentro de una misma estructura, situación que puede dificultar:

- su monitoreo;
- trazabilidad;
- evaluación de efectividad;
- y seguimiento frente al riesgo residual.

De igual manera, en ciertos casos las actividades descritas se encuentran orientadas principalmente a tareas operativas o administrativas, sin definir de manera suficientemente clara la acción concreta de control orientada a prevenir, detectar o mitigar el riesgo de corrupción identificado.

En términos generales, los controles revisados evidencian alineación parcial con los lineamientos metodológicos definidos en la Guía V7 y el enfoque SIGRIP; no obstante, se identifican oportunidades de fortalecimiento frente a:

- simplificación metodológica;
- definición de indicadores de seguimiento;
- trazabilidad documental;
- manejo de desviaciones;
- y evaluación de efectividad de controles asociados a riesgos de corrupción e integridad pública.

Adicionalmente, considerando las particularidades operativas y presupuestales de la Secretaría Distrital de Gobierno, especialmente frente al alcance territorial de las Alcaldías Locales y la administración de los Fondos de Desarrollo Local – FDL, se hace necesario fortalecer controles asociados a:

- contratación pública;
- supervisión contractual;
- gestión documental;
- publicación de información;
- manejo de recursos públicos;
- y trazabilidad de actuaciones administrativas en el Nivel Local.

Lo anterior cobra especial relevancia considerando que los Fondos de Desarrollo Local administran recursos públicos superiores a los dos billones de pesos, situación que implica mayores niveles de exposición frente a riesgos asociados a:

- corrupción;
- conflictos de interés;
- direccionamiento indebido;
- riesgos fiscales;
- y afectaciones reputacionales.

En consecuencia, se recomienda fortalecer el acompañamiento metodológico adelantado por la segunda línea de defensa, promoviendo controles más claros, específicos, trazables y alineados con los lineamientos

establecidos en la Guía V7, incorporando adicionalmente un enfoque diferencial para el Nivel Local y los Fondos de Desarrollo Local conforme a su complejidad operativa, administrativa y presupuestal.

### 7.2.3.5. Valoración Riesgo Inherente / Riesgo Residual

A continuación, se presenta los resultados del análisis de la calificación del riesgo inherente en comparación con el riesgo residual, desagregados por proceso:

Tabla 20. Análisis riesgo inherente Vrs. Riesgo Residual

TIPO DE PROCESO	PROCESO	CANTIDAD DE RIESGOS	CALIFICACIÓN RIESGO INHERENTE				CANTIDAD DE CONTROLES	CALIFICACIÓN RIESGO RESIDUAL				TRATAMIENTO		
			EXT	ALT	MOD	BAJ		EXT	ALT	MOD	BAJ	ACE	RED	ELI
ESTRATÉGICO	Planeación Institucional	2	0	2	0	0	3	0	3	0	0	0	3	0
	Comunicación Estratégica	1	1	0	0	0	2	0	1	0	0	0	1	0
	Gestión Patrimonio Documental	1	0	1	0	0	1		1	0	0	0	1	0
	Gerencia de TIC	1	1	0	0	0	1	0	1	0	0	0	1	0
	Planeación y Gestión Sectorial	2	0	2	0	0	4	0	2	0	0	0	2	0
MISIONAL	Relaciones Estratégicas	1	0	1	0	0	1	0	1	0	0	0	1	0
	Convivencia y Diálogo Social	2	2	0	0	0	2	0	2	0	0	0	2	0
	Inspección Vigilancia y Control	1	0	1	0	0	1	0	1	0	0	0	1	0
	Fomento y Protección de Derechos Humanos	1	0	1	0	0	1	0	1	0	0	0	1	0
	Fomento y Protección de los Derechos Étnicos	1	0	1	0	0	1	0	1	0	0	0	1	0
	Acompañamiento a la Gestión Local	1	0	1	0	0	1	0	1	0	0	0	1	0
APOYO	Gerencia del Talento Humano	2	0	2	0	0	2	0	2	0	0	0	2	0
	Gestión Jurídica	1	0	1	0	0	1	0	1	0	0	0	1	0

TIPO DE PROCESO	PROCESO	CANTIDAD DE RIESGOS	CALIFICACIÓN RIESGO INHERENTE				CANTIDAD DE CONTROLES	CALIFICACIÓN RIESGO RESIDUAL				TRATAMIENTO		
			EXT	ALT	MOD	BAJ		EXT	ALT	MOD	BAJ	ACE	RED	ELI
	Gestión Corporativa Institucional	6	0	6	0	0	8	0	6	0	0	0	6	0
	Control Disciplinario	1	1	0	0	0	1	1	0	0	0	0	1	0
EVALUACIÓN Y MEJORA	Evaluación Independiente	1	0	0	1	0	2	0	0	1	0	0	1	0
	Gestión del Conocimiento	4	0	3	1	0	4	0	3	1	0	0	4	0
TRANSVERSAL	Servicio a la Ciudadanía	1	1	0	0	0	4	1	0	0	0	0	1	0
	<b>1 mapa de riesgos</b>	<b>30</b>	<b>6</b>	<b>22</b>	<b>2</b>	<b>0</b>	<b>41</b>	<b>2</b>	<b>27</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>31</b>	<b>0</b>

Fuente: Elaboración propia OCI con base en reporte de la OAP

Del total de 30 riesgos evaluados en su nivel inherente, se identificó que 6 riesgos (20 %) se clasifican como extremos, 22 (73.3 %) como altos y 2 (6.6%) como moderados.

El análisis comparativo entre el riesgo inherente y el riesgo residual permite determinar el grado de efectividad de los controles implementados en los diferentes procesos de la entidad. A partir de este análisis, se evidencia que dos (2) de los riesgos clasificados como extremos mantienen la misma categoría posterior a la aplicación de los controles.

Estos riesgos corresponden a los procesos de Control Disciplinario y Servicio a la Ciudadanía. En el primer caso, se refiere a la posibilidad de afectación reputacional por proferir decisiones disciplinarias contrarias a derecho en beneficio del sujeto procesal o de un interés particular. En el segundo caso, al riesgo asociado a la orientación con calidad y oportunidad a los ciudadanos, así como a la atención de peticiones, quejas, reclamos, sugerencias, consultas, denuncias por actos de corrupción.

Lo anterior evidencia oportunidades de fortalecimiento frente al diseño, implementación y monitoreo de controles asociados a riesgos de corrupción clasificados en zonas de criticidad extrema y alta, particularmente en aquellos casos donde la valoración residual permanece en niveles elevados posterior a la aplicación de controles.

En este sentido, resulta necesario revisar y fortalecer los mecanismos de control y seguimiento implementados, con el propósito de fortalecer la mitigación del riesgo y reducir los niveles de exposición frente a posibles afectaciones:

- reputacionales;
- administrativas;

- disciplinarias;
- fiscales;
- y jurídicas para la Entidad

Así mismo, la revisión de las opciones de tratamiento definidas para los diferentes riesgos evidencia oportunidades de fortalecimiento frente a:

- seguimiento del riesgo residual;
- evaluación periódica de controles;
- y análisis de efectividad de las medidas implementadas.

En consecuencia, se recomienda fortalecer las estrategias de mitigación y monitoreo, revisando la pertinencia de los controles establecidos y promoviendo mecanismos orientados a disminuir tanto la probabilidad como el impacto de los riesgos identificados.

#### 7.2.3.6. Resultados del Monitoreo

La Oficina de Control Interno recibió por parte de la Oficina Asesora de Planeación tres informes cuatrimestrales correspondientes a la vigencia 2025, en los cuales se consolidan los resultados del monitoreo efectuado a los riesgos de gestión y corrupción del Nivel Central y Nivel Local.

De acuerdo con la información reportada, durante la vigencia se materializaron dieciocho (18) riesgos, de los cuales:

- dieciséis (16) corresponden a riesgos de gestión;
- y dos (2) a riesgos de corrupción

A continuación, se presenta la relación de los riesgos de corrupción materializados durante la vigencia 2025:

Tabla 21. Relación Riesgos de Corrupción Materializados

RIESGOS DE CORRUPCIÓN MATERIALIZADOS - 2025				
CUATRIMESTRE	ALCALDÍA	PROCESO	RIESGO	OBSERVACIONES OCI
2do Cuatrimestre	Chapinero	Gestión Corporativa Institucional	Posibilidad de afectación reputacional por omisión o inoportuna divulgación/publicación de información sobre la gestión contractual en las plataformas de contratación pública, limitando el conocimiento a la ciudadanía por beneficiar a un particular	De acuerdo con la información suministrada en el informe de monitoreo no se reporta formulación de plan de mejoramiento interno.

RIESGOS DE CORRUPCIÓN MATERIALIZADOS - 2025				
CUATRIMESTRE	ALCALDÍA	PROCESO	RIESGO	OBSERVACIONES OCI
3er Cuatrimestre	Tunjuelito	Gestión Patrimonio Documental	Posibilidad de afectación reputacional por la pérdida, manipulación o alteración intencional de la información y de los expedientes físicos de los procesos, para beneficio propio o de particulares	De acuerdo con la información suministrada en el informe de monitoreo no se reporta formulación de plan de mejoramiento interno.
<b>TOTAL, RIESGOS MATERIALIZADOS</b>			<b>2</b>	

Fuente: Elaboración propia OCI con base en reporte de la OAP

En las políticas de operación establecidas en el procedimiento PLE-PIN-P015 Administración y Monitoreo de Riesgos de Gestión y Corrupción, se establece que es responsabilidad de cada líder de proceso y/o alcalde local formular los respectivos planes de mejoramiento cuando se evidencie la materialización de riesgos.

No obstante, en el seguimiento realizado por la OCI a la información aportada por la OAP y a los monitoreos efectuados durante la vigencia, no se evidenció soporte documental asociado a la formulación de planes de mejoramiento frente a los riesgos de corrupción materializados en las Alcaldías Locales relacionadas en los informes de monitoreo.

En consecuencia, la ausencia de formulación de planes de mejoramiento frente a la materialización de riesgos, así como la falta de soportes que evidencien el reporte oportuno de posibles eventos de corrupción ante las autoridades competentes, genera debilidades en la gestión institucional del riesgo y en la capacidad de respuesta frente a eventos críticos.

Esta situación podría derivar en la reiteración de las causas que originan los riesgos, la disminución de la efectividad de los controles implementados y el incremento de la probabilidad de ocurrencia de eventos similares. Adicionalmente, expone a la entidad a posibles afectaciones de tipo disciplinario, fiscal, penal y reputacional, al no garantizarse la adopción oportuna de las acciones correctivas y de reporte establecidas en el procedimiento.

En consecuencia, se recomienda fortalecer los mecanismos institucionales de monitoreo y seguimiento frente a riesgos de corrupción materializados, especialmente en el Nivel Local y en los procesos asociados a la administración de los Fondos de Desarrollo Local – FDL, considerando su complejidad operativa, contractual y presupuestal.

Así mismo, resulta necesario fortalecer:

- la formulación de planes de mejoramiento;
- el seguimiento del riesgo residual;
- la trazabilidad documental;
- y los mecanismos de reporte y escalamiento frente a posibles eventos asociados a corrupción e integridad pública,

conforme a los lineamientos definidos en la Guía V7 y el enfoque SIGRIP.

#### 7.2.4. Riesgos de Tipo Fiscal

Si bien el Manual de Gestión del Riesgo (Código: PLE-PIN-M001, Versión 09) incorpora referencias conceptuales asociadas a riesgos fiscales, durante la revisión realizada por la Oficina de Control Interno no se evidenció una metodología estructurada, diferenciada e integral para su gestión a lo largo de las etapas del ciclo del riesgo, esto es: identificación; análisis; valoración; tratamiento; monitoreo; y seguimiento.

En particular, no se observaron: lineamientos metodológicos específicos; criterios técnicos de valoración; tipologías de riesgo fiscal; mecanismos diferenciados de monitoreo; ni herramientas institucionales orientadas a la administración sistemática de riesgos asociados a posibles afectaciones al patrimonio público y detrimento fiscal.

Así mismo, no se evidenciaron matrices o instrumentos formales en los cuales los riesgos fiscales se encuentren: identificados; clasificados; valorados; y monitoreados, incorporando elementos asociados a: causas; consecuencias; controles; responsables; riesgo residual; y acciones de tratamiento.

Lo anterior limita la capacidad institucional para: anticipar; prevenir; monitorear; y mitigar eventos con potencial afectación sobre los recursos públicos, así como fortalecer mecanismos de prevención del daño patrimonial y toma oportuna de decisiones frente a riesgos asociados a la gestión fiscal.

Adicionalmente, se identifican oportunidades de fortalecimiento frente a la articulación entre la política institucional de gestión del riesgo y los lineamientos asociados al control fiscal, particularmente frente a riesgos derivados de: contratación pública; supervisión e interventoría; ejecución presupuestal; gestión documental; pago de obligaciones; administración de bienes y recursos públicos; gestión de proyectos de inversión; y cumplimiento de metas financiadas con recursos públicos.

Este aspecto cobra especial relevancia considerando las particularidades operativas y presupuestales de la Secretaría Distrital de Gobierno y el alcance territorial de las Alcaldías Locales y los Fondos de Desarrollo Local – FDL, los cuales administran recursos públicos superiores a los dos billones de pesos destinados principalmente a: contratación e inversión local; infraestructura; fortalecimiento institucional; participación ciudadana; convivencia y seguridad; y ejecución de proyectos territoriales.

En este contexto, la ausencia de una metodología diferencial para riesgos fiscales podría limitar la identificación temprana de eventos asociados a: posibles detrimentos patrimoniales; debilidades en supervisión contractual; incumplimientos contractuales; pagos sin soporte; deficiencias en ejecución presupuestal; riesgos asociados a reservas y pasivos; y demás situaciones con impacto fiscal para la Entidad y los Fondos de Desarrollo Local.

Así mismo, se identifican oportunidades de fortalecimiento frente a: incorporación de riesgos fiscales dentro de las matrices institucionales; definición de controles preventivos y detectivos específicos; articulación con las líneas de defensa; monitoreo diferencial para el Nivel Local; y consolidación de mecanismos de seguimiento orientados a la prevención del daño patrimonial.

En consecuencia, se recomienda fortalecer la Política Integral de Gestión del Riesgo incorporando un componente metodológico específico para la gestión de riesgos fiscales, alineado con:

- la Guía para la Gestión Integral del Riesgo V7;

- la Ley 610 de 2000;
- el enfoque preventivo del control fiscal;
- y las particularidades administrativas, operativas, contractuales y presupuestales de la Secretaría Distrital de Gobierno y los Fondos de Desarrollo Local.

### 7.2.5. Seguimiento a las recomendaciones del informe 2025.

En el marco del seguimiento efectuado a las recomendaciones formuladas en el informe de gestión del riesgo correspondiente a la vigencia 2025, la Oficina Asesora de Planeación – OAP suministró información relacionada con las acciones adelantadas frente a las oportunidades de mejora identificadas por la Oficina de Control Interno.

Tabla 22. Seguimiento a las recomendaciones 2025

No.	Recomendación 2025	Plan de acción implementado / avance
1	Diseñar e implementar un enfoque descentralizado y contextualizado para la gestión del riesgo en el nivel local.	Se adelantan acciones conjuntas entre OAP, SGI y DTI; socialización de lineamientos con Alcaldías Locales e identificación de riesgos por localidad.
2	Fortalecer el cumplimiento del Manual GCN-M002 y formulación de planes de mejoramiento.	Se realizan monitoreos cuatrimestrales, generación de alertas y socialización de resultados en el CIGD.
3	Establecer responsabilidades administrativas y acciones correctivas frente a incumplimientos.	Actualización del Manual de Gestión del Riesgo y definición de responsabilidades y líneas de defensa.
4	Eliminar celdas ocultas y estandarizar formatos.	Se estandarizaron formatos y se avanza en parametrización del módulo de riesgos en la plataforma MATIZ.
5	Institucionalizar mecanismos de validación por parte de la OAP.	Se implementaron carpetas compartidas y herramientas para cargue y seguimiento de monitoreos de riesgos.
6	Realizar jornadas permanentes y obligatorias de capacitación.	Se realizaron capacitaciones y socializaciones metodológicas dirigidas a promotores de mejora y procesos.
7	Evaluar e implementar controles automáticos en procesos clave.	La implementación corresponde a líderes de proceso y Alcaldías Locales como primera línea de defensa.
8	Reforzar controles correctivos y planes de contingencia.	La gestión y fortalecimiento de controles quedó a cargo de líderes de proceso y Alcaldías Locales.
9	Realizar análisis causa-raíz de riesgos materializados.	Se indicó responsabilidad de líderes de proceso y Alcaldías Locales para su implementación.
10	Actualizar periódicamente el mapa de riesgos y verificar efectividad de controles.	Actividad asignada a procesos y Alcaldías Locales dentro de la gestión de monitoreo y actualización.
11	Fortalecer el rol de la OAP en seguimiento y monitoreo.	La OAP realiza acompañamiento metodológico y seguimiento general a riesgos institucionales.
12	Incorporar nuevas tipologías de riesgo.	Se adelanta actualización del Manual de Gestión del Riesgo incorporando nuevas tipologías.
13	Definir procedimiento para identificar y gestionar riesgos emergentes.	Actividad incluida dentro de la actualización metodológica del Manual de Gestión del Riesgo.

Fuente: Elaboración propia OCI con base en reporte de la OAP

## 8. Conclusiones

### 8.1. Conclusiones generales:

- En términos generales, se concluye que la Política de Gestión del Riesgo y el Manual PLE-PIN-M001 V9 incorporan elementos metodológicos alineados con la Guía para la Gestión Integral del Riesgo V7; no obstante, se identifican oportunidades de fortalecimiento frente a componentes estratégicos, de gobernanza, monitoreo y madurez institucional, con el propósito de consolidar una mayor armonización con el enfoque actualizado definido por Función Pública.

- Adicionalmente, resulta necesario considerar las particularidades operativas, administrativas y presupuestales del Nivel Local y de los Fondos de Desarrollo Local – FDL, considerando que las Alcaldías Locales administran recursos públicos superiores a los dos billones de pesos, asociados principalmente a:

- ✓ contratación pública;
- ✓ ejecución presupuestal;
- ✓ inversión territorial;
- ✓ supervisión contractual;
- ✓ participación ciudadana;
- ✓ y gestión administrativa local.

En este contexto, la gestión institucional del riesgo requiere incorporar un enfoque diferencial para el Nivel Local, que permita fortalecer:

- ✓ la identificación y monitoreo de riesgos;
- ✓ la segregación de responsabilidades;
- ✓ los controles asociados a la gestión territorial;
- ✓ y los mecanismos de seguimiento y trazabilidad sobre los recursos administrados por los Fondos de Desarrollo Local

- Como resultado del análisis, se evidenció que la Entidad cuenta con un total de 200 riesgos y 358 controles identificados y distribuidos en 38 mapas de riesgos. Del total de riesgos identificados, el 51% corresponde a riesgos de gestión, el 34% a riesgos de seguridad de la información y el 15% a riesgos de corrupción. No obstante, no se identifican matrices o herramientas formales en las que los riesgos fiscales se encuentren registrados, ni la totalidad de los riesgos asociados a la integridad pública, tales como fraude, inadecuada gestión de conflictos de interés, así como aquellos relacionados con el lavado de activos, la financiación del terrorismo y la proliferación de armas de destrucción masiva (LA/FT/FP), lo que evidencia oportunidades de fortalecimiento en la cobertura y metodología integral del sistema de administración del riesgo.
- En cuanto a las herramientas para la gestión del riesgo, la Entidad cuenta con manuales, procedimientos y formatos institucionales, así como con 38 mapas de riesgos distribuidos en gestión, seguridad de la información y corrupción. No obstante, se evidencia que la gestión de los riesgos de seguridad de la información no se encuentra plenamente integrada a la política institucional, ya que se desarrolla de manera autónoma desde la Dirección de Tecnologías de la Información, sin articulación metodológica con los demás instrumentos de gestión del riesgo. En consecuencia, se requiere fortalecer su formalización e integración para asegurar un enfoque integral del sistema de administración del riesgo.

## 8.2. Conclusiones Riesgos de gestión:

- El análisis permite concluir que, aunque los procesos han identificado riesgos relevantes para la gestión institucional, persisten debilidades importantes en su formulación técnica y metodológica. La principal oportunidad de mejora consiste en fortalecer la construcción de riesgos bajo un enfoque integral que contemple de manera clara las causas, el evento y las consecuencias, permitiendo así una mejor valoración, monitoreo y definición de controles.

- Se evidencian oportunidades de mejora en la identificación, diseño e implementación de los controles existentes, dado que la permanencia de riesgos en nivel extremo y la continuidad de más de la mitad de los riesgos en nivel alto en la misma categoría sugieren que los controles aplicados no están siendo suficientemente efectivos para mitigar los riesgos de mayor criticidad. En este sentido, se requiere revisar y fortalecer los controles establecidos, con el fin de asegurar una mitigación efectiva y una reducción real del nivel de exposición al riesgo.
- En el seguimiento realizado se evidenció que, de los 16 riesgos de gestión materializados en la vigencia 2025, el 61,1 % corresponde al Nivel Local y el 38,9 % al Nivel Central, lo que refleja una mayor incidencia en el ámbito territorial. Asimismo, solo 6 riesgos cuentan con plan de acción implementado, lo cual evidencia incumplimiento del procedimiento PLE-PIN-P015, que establece la obligación de cada líder de proceso y/o alcalde local de formular e implementar acciones de mejora ante la materialización de riesgos. En consecuencia, se identifican debilidades en la gestión oportuna de acciones correctivas, lo que puede afectar la efectividad del sistema de administración del riesgo.
- El análisis de los tres (3) riesgos materializados con mayor recurrencia durante la vigencia 2025 evidencia la persistencia de debilidades en la oportunidad de respuesta a los derechos de petición, la coordinación institucional y la gestión territorial, con especial incidencia en el proceso de Servicio a la Ciudadanía, donde se concentra el mayor número de eventos y planes de acción. Asimismo, se observa que en algunos casos no se ha logrado el cierre oportuno ni la implementación efectiva de acciones correctivas, lo que refleja posibles debilidades en la efectividad de los controles y en el seguimiento a los planes de mejora, afectando la capacidad institucional para prevenir la recurrencia de los eventos y fortalecer la gestión oportuna y eficiente.

### 8.3. Conclusiones Riesgos de Seguridad de la Información

- La entidad cuenta con instrumentos metodológicos y documentales para la gestión de riesgos de Seguridad de la Información, alineados con el Manual PLE-PIN-M001 V9, el procedimiento PLE-PIN-P017 y el Modelo de Seguridad y Privacidad de la Información; sin embargo, las matrices revisadas se encuentran en construcción y no cuentan con formalización mediante fecha y versión aprobada.
- Se evidenció una implementación parcial de la gestión de riesgos de Seguridad de la Información, debido a que no todas las dependencias y Alcaldías Locales cuentan con matrices formuladas, identificándose únicamente cinco (5) Alcaldías Locales con riesgos documentados, situación que limita la cobertura integral del modelo institucional.
- Aunque los riesgos identificados cuentan principalmente con controles preventivos y mecanismos de monitoreo definidos, no se evidenciaron suficientes soportes, trazabilidad ni validación independiente sobre la ejecución y efectividad de los controles implementados, especialmente en lo relacionado con el esquema de líneas de defensa.
- El análisis realizado evidenció oportunidades de mejora en la integración institucional de la gestión de riesgos de Seguridad de la Información, particularmente en la articulación metodológica con la política integral de riesgos, el fortalecimiento del monitoreo, la formalización de matrices y la implementación homogénea en todos los procesos y niveles de la entidad.

#### 8.4. Conclusiones Riesgos de Corrupción:

- En términos generales, la mayoría de los riesgos evaluados cumplen parcialmente con la estructura metodológica establecida en la Guía para la Administración del riesgo V7, particularmente en lo relacionado con la identificación del impacto asociado al riesgo. No obstante, persisten debilidades en la definición de la causa inmediata y la causa raíz, ya que, aunque se describe de manera clara el impacto reputacional, no se identifican con precisión los factores o condiciones que podrían generar la materialización del riesgo, lo que limita el análisis integral del mismo y dificulta la adecuada definición de controles preventivos y acciones de mitigación efectivas.
- Se identifican oportunidades de fortalecimiento frente al diseño, implementación y monitoreo de los controles existentes, considerando que la permanencia de riesgos en nivel extremo y la continuidad de varios riesgos en nivel alto dentro de la misma categoría residual evidencian necesidad de fortalecer los mecanismos de mitigación y seguimiento frente a riesgos de mayor criticidad.
- En los informes de monitoreo aportados por la Oficina Asesora de Planeación (OAP) se reporta la materialización de dos (2) riesgos de corrupción en el Nivel Local; sin embargo, no se evidencia la formulación de planes de mejoramiento conforme a lo establecido en el procedimiento institucional, ni el cumplimiento de la obligación de reportar de manera oportuna estos eventos ante los entes de control competentes. En consecuencia, esta situación evidencia debilidades en la gestión institucional del riesgo y en la capacidad de respuesta oportuna frente a la materialización de eventos de corrupción.

### 9. Recomendaciones

#### 9.1. Recomendaciones generales

- Fortalecer la alineación de la Política de Gestión del Riesgo con la Guía para la Gestión Integral del Riesgo V7, mediante la revisión y actualización del documento PLE-PIN-M001 V9. Este ajuste debe garantizar la incorporación integral de los lineamientos establecidos en la guía, particularmente en lo relacionado con el análisis del contexto interno y externo, la promoción de una cultura organizacional del riesgo, el enfoque de integridad pública, los mecanismos de comunicación y reporte, así como la implementación de acciones de mejora continua del sistema de gestión del riesgo. Lo anterior permitirá consolidar una política más robusta, coherente y alineada con las mejores prácticas en la materia.
- Fortalecer el enfoque diferencial y territorial de la política de gestión del riesgo, de manera que cada Alcaldía Local, en su calidad de unidad operativa con particularidades propias, cuente con la capacidad efectiva para identificar, analizar, gestionar y monitorear sus riesgos de forma integral, conforme a su contexto territorial, operativo y administrativo. En este sentido, se sugiere promover la elaboración de matrices de riesgo específicas para cada localidad, evitar la réplica automática de los riesgos definidos en el Nivel Central, fortalecer la participación activa de las Alcaldías Locales en la formulación, seguimiento y control de sus riesgos, y consolidar lineamientos claros que permitan diferenciar adecuadamente los riesgos y las responsabilidades entre el Nivel Central y el Nivel Local, garantizando una gestión del riesgo más precisa, pertinente y ajustada a las realidades institucionales.

- Se recomienda a la Entidad definir una metodología de gestión integral del riesgo, con el fin de garantizar una identificación más completa y sistemática de los riesgos institucionales. En este sentido, resulta pertinente incorporar de manera explícita los riesgos de tipo fiscal y aquellos asociados a la integridad pública, tales como fraude, inadecuada gestión de conflictos de interés, así como los relacionados con el lavado de activos, la financiación del terrorismo y la proliferación de armas de destrucción masiva (LA/FT/FP). Lo anterior permitirá ampliar el alcance del sistema, asegurar una gestión más integral y robusta, y fortalecer la capacidad institucional para la prevención, detección y tratamiento oportuno de los riesgos.
- Articular e integrar la gestión de los riesgos de seguridad de la información dentro de la política institucional de administración del riesgo, de manera que no se gestione de forma autónoma por la Dirección de Tecnologías de la Información, sino que se encuentre plenamente alineada con los manuales, procedimientos y demás instrumentos existentes. En este sentido, es necesario formalizar su incorporación metodológica al sistema de gestión del riesgo, garantizando coherencia, trazabilidad y un enfoque integral que permita una adecuada identificación, análisis, tratamiento y seguimiento de todos los tipos de riesgo institucionales.

## **9.2. Recomendaciones Riesgos de Gestión:**

- Fortalecer la formulación técnica y metodológica de los riesgos institucionales, de manera que su construcción se realice bajo un enfoque integral que permita identificar de forma clara y coherente las causas, el evento y las consecuencias asociadas. Lo anterior contribuirá a mejorar la calidad del análisis del riesgo, facilitar su adecuada valoración y monitoreo, y asegurar la definición de controles más efectivos y orientados a la prevención y mitigación de su materialización.
- Revisar y fortalecer la identificación, diseño e implementación de los controles asociados a los riesgos institucionales, considerando que la permanencia de riesgos en nivel extremo y la continuidad de más de la mitad de los riesgos en nivel alto dentro de la misma categoría evidencian posibles debilidades en su efectividad para la mitigación de los riesgos de mayor criticidad. En este sentido, es necesario ajustar y optimizar los controles existentes, con el propósito de asegurar una mitigación efectiva, reducir de manera real el nivel de exposición al riesgo y fortalecer el sistema de control interno de la Entidad.
- Fortalecer la gestión de los riesgos materializados, con especial énfasis en el Nivel Local, considerando la mayor incidencia identificada en este ámbito durante la vigencia 2025. En este sentido, es necesario garantizar el cumplimiento del procedimiento PLE-PIN-P015, asegurando que cada líder de proceso y/o alcalde local formule e implemente de manera oportuna los planes de acción correspondientes ante la materialización de riesgos. Lo anterior permitirá mejorar la oportunidad y efectividad de las acciones correctivas, así como fortalecer el Sistema de Administración del Riesgo y reducir la probabilidad de recurrencia de eventos similares.
- Para la gestión de los riesgos materializados con mayor recurrencia se recomienda revisar y fortalecer la efectividad de los controles existentes, así como garantizar el seguimiento oportuno, cierre efectivo y evaluación de los planes de acción derivados de la materialización. Lo anterior permitirá mejorar la capacidad institucional para prevenir la recurrencia de los eventos, fortalecer la gestión oportuna y eficiente, y promover la mejora continua en los procesos.

**9.3. Recomendaciones Riesgos de Seguridad de la Información**

- Formalizar y aprobar las matrices de riesgos de Seguridad de la Información, asegurando que cuenten con versión, fecha de adopción, responsables definidos y trazabilidad documental conforme a los lineamientos institucionales y la Guía para la Gestión Integral del Riesgo V7.
- Fortalecer la implementación institucional de la gestión de riesgos de Seguridad de la Información en todas las dependencias y Alcaldías Locales, garantizando una cobertura integral y homogénea de identificación, valoración, tratamiento y monitoreo de riesgos.
- Fortalecer los mecanismos de seguimiento, monitoreo independiente y validación de controles bajo el esquema de líneas de defensa, asegurando la generación de evidencias, trazabilidad y evaluación de efectividad de los controles implementados.
- Integrar de manera armonizada la gestión de riesgos de Seguridad de la Información con la política institucional de gestión del riesgo y el MSPI, fortaleciendo los lineamientos metodológicos, el análisis de contexto y la mejora continua.

**9.4. Recomendaciones Riesgos de Corrupción**

- Fortalecer la formulación de los riesgos institucionales en el marco de la Guía para la Administración del Riesgo V7, con el fin de garantizar el cumplimiento integral de la estructura metodológica establecida. En este sentido, es necesario profundizar en la identificación de la causa inmediata y la causa raíz, asegurando que no solo se describa el impacto reputacional, sino que también se identifiquen con precisión los factores o condiciones que pueden originar la materialización del riesgo. Lo anterior permitirá mejorar el análisis integral de los riesgos y facilitar la definición de controles preventivos y acciones de mitigación más efectivas y pertinentes.
- Revisar y fortalecer los controles establecidos, con el fin de garantizar una mitigación efectiva y una reducción real del nivel de exposición al riesgo, considerando que la falta de resultados significativos en la disminución de los riesgos críticos podría generar posibles afectaciones económicas y/o reputacionales para la Entidad, lo que hace necesaria la adopción prioritaria de acciones de mejora y estrategias de fortalecimiento del sistema de control.
- Fortalecer el cumplimiento del procedimiento institucional frente a la gestión de riesgos de corrupción materializados, garantizando que, una vez identificados eventos en el Nivel Local, se formulen de manera oportuna los respectivos planes de mejoramiento y se realicen los reportes correspondientes ante los entes de control competentes, según aplique. Lo anterior, con el fin de asegurar la adopción de las acciones administrativas, disciplinarias, fiscales o penales a que haya lugar, así como fortalecer la capacidad de respuesta institucional frente a la materialización de este tipo de riesgos.

La Oficina de Control Interno recomienda fortalecer el Sistema Integral de Gestión del Riesgo de la Entidad mediante la consolidación de metodologías homogéneas, mecanismos de monitoreo diferencial, evaluación de efectividad de controles y fortalecimiento del enfoque preventivo, incorporando de manera prioritaria las particularidades operativas, contractuales, territoriales y presupuestales del Nivel Local y de los Fondos de Desarrollo Local – FDL, conforme a los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo V7 y las políticas institucionales de control interno y gobernanza.

(ORIGINAL FIRMADO)

Elaborado por		Revisado y Aprobado por	
<b>Deissy Liliana Sotelo Torres</b> Professional contratista – Oficina de Control Interno			
<b>Yeina Rocio Aviles Barreiro</b> Professional contratista – Oficina de Control Interno		<b>Lady Johanna Medina Murillo</b> Jefe Oficina de Control Interno.	
<b>Fecha:</b>	29/05/2026	<b>Fecha:</b>	29/05/2026