POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

2026

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

Contenido

1. OBJETIVO 4
2. PRINCIPIOS ORIENTADORES DE LA GESTIÓN INTEGRAL DEL RIESGO....5
3. DEFINICIONES Y MARCO CONCEPTUAL 5
4. MARCO NORMATIVO 9
5. ALCANCE....10
6. COMPROMISO 11
7. ROLES Y RESPONSABILIDADES....15
8. GUÍAS DE ACCIÓN, DISEÑO Y PLANEACIÓN....18
9.1. Niveles de severidad del riesgo 18
9.2. Tratamiento del riesgo 20
10. MANEJO DE RIESGOS MATERIALIZADOS....21
10.1. Gestión de eventos materializados 21
10.1.1. Obligatoriedad del reporte periódico....21
10.1.2. Reporte inmediato de eventos de riesgo 22
10.2. Procedimiento 22
10.2.1 Etapas Mínimas del Proceso....22
10.2.2. Asignación de Responsabilidades 22
10.2.3. Registro y Trazabilidad....23
10.2.4. Clasificación del evento 23
10.2.5. Tiempos de gestión....23
10.2.6. Escalamiento....23
10.2.7. Articulación con la gestión de riesgos 23
10.2.8. Seguimiento y control 23
10.2.9. Comunicación y confidencialidad 23
10.3. Acciones específicas por tipología de riesgo 24
10.3.1. Riesgos de Integridad, ...24
10.3.2. Riesgos relacionados con lavado de activos y financiación del terrorismo - LA/FT/FPADM:....25
10.3.3. Riesgos de gestión, ambientales y de seguridad digital 27
10.4. Actividades para la identificación y la gestión de riesgos desde la primera línea 27
10.4.1. Identificación, Análisis y Evaluación (Planear / Diseñar) 28
10.4.2. Monitoreo y Ejecución de Controles (Hacer / Implementar) 28
10.4.3. Períodos de Revisión y Mesa de Trabajo (Verificar / Evaluar)....28
10.4.4. Monitoreo de Segunda Línea y Seguimiento de Tercera Línea (Aseguramiento)....29

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

10.4.5. Gestión ante la Materialización de Riesgos (Actuar / Ajustar) 29
11. MONITOREO, EVALUACIÓN Y SEGUIMIENTO DE LA GESTIÓN DE RIESGOS 29
11.1. Gestión y autocontrol – Primera Línea de Defensa 29
11.2. Monitoreo – Segunda Línea de Defensa 29
11.3. Evaluación independiente – Tercera Línea de Defensa 30
12. FUENTES Y BIBLIOGRAFÍA 30

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

1. INTRODUCCIÓN

En el contexto de la implementación del Modelo Integrado de Planeación y Gestión (MIPG), Canal Capital se compromete a establecer y fortalecer sus políticas de gestión para garantizar la sostenibilidad y transparencia en todas sus operaciones. Esta iniciativa surge como respuesta a la necesidad de abordar diversos aspectos que afectan la integridad y eficiencia de la entidad, considerando los riesgos de gestión, de integridad —incluyendo el lavado de activos, la financiación del terrorismo y la proliferación de armas de destrucción masiva (LA/FT/PADM) y las amenazas de corrupción—, así como los riesgos de gestión, ambientales, fiscales y de seguridad digital, entre otros.

La gestión de riesgos adquiere un papel fundamental en el diseño e implementación de estrategias que salvaguarden los intereses de Canal Capital y su compromiso con la ética y la responsabilidad social. A través de este documento de política de administración de riesgos, la entidad se propone orientar y guiar la identificación, evaluación, manejo, análisis y valoración de posibles amenazas que detonen vulnerabilidades institucionales, estableciendo mecanismos efectivos bajo el enfoque de la prevención y mitigación de situaciones adversas. En este marco, Canal Capital reafirma su compromiso con las mejores prácticas de gobierno corporativo y la mejora continua, asegurando un manejo responsable y eficiente de los riesgos asociados a sus operaciones; de esta manera, la gestión integral del riesgo contribuirá a la protección, sostenibilidad y generación de valor público, fortaleciendo la confianza ciudadana, la continuidad institucional y la adecuada prestación del servicio público de televisión regional, lo cual constituye uno de los principales objetivos de la administración del riesgo.

La integración de estas dimensiones en la estrategia general de gestión de riesgos permitirá a Canal Capital fortalecer su posición como una entidad confiable y responsable, alineada con los principios y directrices del SIGRIP. Este documento servirá como guía para los directivos, colaboradores y grupos de valor de la empresa, proporcionando un marco claro y estructurado para la toma de decisiones que garantice la sostenibilidad y el cumplimiento de los objetivos institucionales.

2. OBJETIVO

Establecer los lineamientos y criterios para la gestión integral del riesgo en Canal Capital, orientados a identificar, analizar, evaluar, tratar, monitorear, comunicar y revisar los riesgos que puedan afectar el cumplimiento de la misión, los objetivos estratégicos institucionales, la continuidad de la operación y la generación de valor público. Asimismo, definir el marco de apetito, tolerancia y capacidad de riesgo de la Entidad. Así como los mecanismos de articulación con el MIPG, el SIGRIP y los demás instrumentos institucionales de planeación, control y seguimiento, en concordancia con los principios de integridad, transparencia, mejora continua, planeación eficiente y toma de decisiones basada en riesgos[1].

[1] La presente política adopta el marco de Gestión Integral del Riesgo, alineado con el MIPG y los estándares COSO-ERM (2017) e ISO 31000:2018, con el fin de fortalecer el buen gobierno, la transparencia y la creación de valor público.

1. PRINCIPIOS ORIENTADORES DE LA GESTIÓN INTEGRAL DEL RIESGO

Para fortalecer la estructura conceptual y metodológica de la presente política, así como su alineación con las buenas prácticas de gobernanza pública, la gestión integral del riesgo en Canal Capital se fundamenta en los siguientes principios orientadores:

Enfoque preventivo: Priorización de la identificación y mitigación oportuna de los riesgos antes de su materialización, minimizando impactos adversos en la operación.

Mejora continua: Evaluación constante y actualización periódica de los mecanismos de control y administración del riesgo para adaptarlos al entorno institucional y tecnológico.

Transparencia: Disposición y acceso público a la información sobre la gestión de riesgos, promoviendo la rendición de cuentas y la integridad.

Trazabilidad: Garantía de que cada etapa del proceso de gestión del riesgo sea registrable, verificable y auditable a lo largo del tiempo.

Coordinación institucional: Articulación armónica entre las diferentes áreas, líneas de defensa y colaboradores para asegurar una respuesta integral ante las amenazas.

Toma de decisiones basada en información: Uso de datos empíricos, métricas y análisis de contexto como insumo técnico y objetivo para la toma de decisiones estratégicas.

Generación de valor público: Orientación de la gestión del riesgo hacia la protección de los recursos, la continuidad institucional y la excelencia en la prestación del servicio público de televisión regional.

2. DEFINICIONES Y MARCO CONCEPTUAL

Para efectos de la presente política, se adoptan las siguientes definiciones, alineadas con las mejores prácticas de gestión del riesgo y los lineamientos del DAFP, MIPG e ISO 31000:

Conceptos generales
Riesgo: Efecto de la incertidumbre sobre el cumplimiento de los objetivos institucionales.

Gestión del riesgo: Proceso estructurado para identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos.

Evento de riesgo: Situación potencial que, de materializarse, puede generar impactos negativos o positivos en la entidad.

Riesgo materializado: Ocurrencia efectiva de un evento de riesgo.

Causa: Factor interno o externo que origina un riesgo.

Causa raíz: Debilidades en la gestión y aplicación de los controles de seguridad de la información.

Causa inmediata: Falta de aplicación de las medidas de seguridad durante el acceso o manejo de la información.

Consecuencia: Resultado derivado de la materialización del riesgo.

Amenazas y vulnerabilidad ante la corrupción: Posibilidad de que, por acción u omisión, se usen las facultades de un cargo o los recursos de la entidad para obtener un beneficio privado (para sí mismo o para un tercero), afectando los intereses de la administración pública.

Impacto reputacional: Posibilidad de afectación negativa, descrédito o pérdida de confianza en la imagen institucional de Canal Capital ante la ciudadanía, grupos de valor o partes interesadas, derivada de la materialización de fallas operativas o conductas indebidas.

Valoración del riesgo
Probabilidad: Posibilidad de ocurrencia del riesgo.

Impacto: Nivel de afectación sobre los objetivos institucionales.

Nivel de riesgo (severidad): Resultado de combinar probabilidad e impacto.

Riesgo inherente: Nivel de riesgo sin considerar controles.

Riesgo residual: Nivel de riesgo posterior a la aplicación de controles.

Límites cualitativos y cuantitativos: Umbrales o baremos establecidos por la entidad para medir y controlar el nivel de exposición al riesgo. Los límites cualitativos definen criterios descriptivos de aceptación, mientras que los cuantitativos fijan rangos numéricos, presupuestales o de frecuencia.

Tratamiento y control
Tratamiento del riesgo: Acciones orientadas a modificar el nivel de riesgo.

Control: Medida implementada para prevenir, detectar o corregir eventos de riesgo.

Aceptar el riesgo: Decisión informada de no implementar controles adicionales dentro del nivel permitido.

Reducir el riesgo: Implementación de controles para disminuir probabilidad o impacto.

Debida diligencia: Validación de información de terceros o contrapartes que incluye medidas para prevenir riesgos de integridad y LA/FT/FPADM.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

Evitar el riesgo: Eliminación de la actividad que genera el riesgo.

Transferir o compartir el riesgo: Asignación parcial del riesgo a un tercero.

Gobierno del riesgo
Apetito de riesgo: Nivel de riesgo que la entidad está dispuesta a asumir.

Tolerancia al riesgo: Margen de variación permitido respecto al apetito.

Capacidad de riesgo: Nivel máximo de riesgo que la entidad puede soportar.

Líneas de defensa: Modelo de responsabilidades para la gestión del riesgo:

Primera línea: Gestión y control operativo del riesgo.

Segunda línea: Supervisión, asesoría y consolidación.

Tercera línea: Evaluación independiente (Control Interno).

Seguimiento y medición

Monitoreo: Revisión continua del comportamiento de los riesgos y controles.

Seguimiento: Evaluación periódica de la gestión del riesgo.

Indicador Clave de Riesgo (KRI): Métrica que permite anticipar cambios en la exposición al riesgo.

Indicador Clave de Desempeño (KPI): Métrica que mide el cumplimiento de objetivos.

Alerta temprana: Señal que indica posibles desviaciones del nivel de riesgo esperado.

Tipologías de riesgo

Riesgos de gestión: Asociados a procesos, proyectos y operación institucional.

Riesgos de integridad: Aquellos asociados a la vulneración de los valores, principios y normas éticas del servicio público, que ocurren cuando el servidor o servidora se desvía de los estándares, y normas institucionales, y que debilitan la confianza ciudadana y los fines del Estado, más allá de constituir o no un delito penal de corrupción.

Riesgos LA/FT/FPADM: Asociados al lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva.

Riesgos de seguridad de la información: Asociados a la confidencialidad, integridad y disponibilidad de la información, infraestructura tecnológica y ciberamenazas.

Riesgos fiscales: Relacionados con la gestión, administración y protección de recursos públicos y patrimoniales.

Riesgos ambientales: Predisposición a sufrir pérdidas o daños de los seres humanos, sus medios de subsistencia, sistemas físicos, económicos y el medio ambiente, al ser afectados por eventos físicos peligrosos (Conforme a la Ley 1523 de 2012, modificada por la Ley 2474 de 2025).

Riesgo legal y de cumplimiento: Posibilidad de pérdidas, sanciones económicas o fallos judiciales adversos debido al incumplimiento de normas legales, reglamentarias, obligaciones contractuales o políticas internas vigentes.

Riesgos de continuidad de negocio: Eventos potenciales que pueden interrumpir de manera parcial o total la operación, afectando la disponibilidad de los servicios esenciales y la transmisión del servicio público de televisión regional.

Gestión de eventos materializados

Detección: Identificación del evento de riesgo.

Contención: Acciones inmediatas para mitigar impactos.

Investigación: Análisis de causas raíz.

Lecciones aprendidas: Resultados del análisis de eventos para fortalecer controles.

Integridad y cumplimiento

Integridad pública: Actuación conforme a principios éticos, transparencia y legalidad.

Lavado de Activos: Conducta consistente en adquirir, administrar, custodiar, transformar, transferir o realizar cualquier operación sobre bienes o recursos provenientes de actividades ilícitas, así como ocultar su origen o darles apariencia de legalidad mediante su incorporación al sistema económico formal. Ver artículo 323 del Código Penal Colombiano.

Financiación del Terrorismo: Conducta consistente en proveer, recolectar, entregar, recibir, administrar, aportar, custodiar o guardar fondos, bienes o recursos, de manera directa o indirecta, o realizar cualquier acto destinado a promover, organizar, apoyar, mantener, financiar o sostener económicamente grupos de delincuencia organizada, grupos armados al margen de la ley, grupos terroristas nacionales o extranjeros o a sus integrantes. Ver artículo 345 del Código Penal Colombiano.

Financiación de la Proliferación de Armas de Destrucción Masiva: acto de proveer fondos o servicios financieros que se utilicen, total o parcialmente, para la fabricación, adquisición, posesión, desarrollo, exportación, transbordo, transporte, almacenamiento o uso de armas nucleares, químicas o biológicas, sus sistemas de lanzamiento y materiales relacionados.

Persona Expuesta Públicamente (PEP): Servidores públicos y particulares que por su cargo,

funciones o el manejo de recursos públicos gozan de notoriedad pública, estando expuestos en mayor medida a riesgos asociados a la corrupción y al lavado de activos.

ROS (Reporte de Operación Sospechosa): Operación que, por su número, cantidad o características, no se enmarca dentro de los sistemas y prácticas normales del negocio o sector y que, de acuerdo con los usos y costumbres de la actividad, no ha podido ser razonablemente justificada.

Riesgos asociados a Inteligencia Artificial
Sesgo algorítmico: Resultado sistemáticamente distorsionado en sistemas de IA.

Human-in-the-loop (Humano en el bucle): Modelo de interacción donde la intervención humana es obligatoria en el ciclo de decisión de un sistema de IA. Implica que una persona debe supervisar, revisar y validar la decisión antes de que esta sea ejecutada o produzca efectos jurídicos o administrativos, actuando como control preventivo ante sesgos o errores.

3. MARCO NORMATIVO

La Política para la Gestión Integral del Riesgo de Canal Capital se fundamenta y alinea con el marco legal, reglamentario y técnico vigente en Colombia en materia de función pública, transparencia, seguridad digital, gestión del riesgo de desastres y prevención de actividades ilícitas, compuesto por:

5.1. Marco General de Gestión Pública y Transparencia

Decreto 1499 de 2017, por medio del cual se actualiza el Modelo Integrado de Planeación y Gestión (MIPG) como marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas.

Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública, y Decreto 1499 de 2017, por medio del cual se modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.Modelo Estándar de Control Interno (MECI): Estructura de control para garantizar el cumplimiento de los objetivos institucionales y la eficiencia en los procesos.

Ley 1712 de 2014 Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Decreto Único Reglamentario 1081 de 2015 Sector Presidencia de la República: Compila las directrices normativas sobre transparencia, acceso a la información pública y debida diligencia, incluyendo las disposiciones del Decreto 103 de 2015.

Resolución 1519 de 2020 del Ministerio de TIC: Define los estándares y directrices para la publicación de información, accesibilidad web y seguridad en medios digitales.

5.2. Marco de Gestión del Riesgo e Integridad Pública

Especialmente la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 7)

Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP): Modelo metodológico enfocado en articular de manera transversal la prevención de fallos éticos y conductas contrarias a la integridad del servicio público.

Catálogo Indicativo de Puntos de Riesgo Fiscal del DAFP: Instrumento de referencia utilizado para la implementación de la Gestión Preventiva de Riesgos Fiscales ante posibles efectos dañosos sobre los recursos patrimoniales del Estado.

Norma ISO 31000: Estándar técnico internacional que proporciona las directrices y principios generales para la gestión estructurada del riesgo.

5.3. Marco de Seguridad Digital y Privacidad de la Información

Decreto Único Reglamentario 1078 de 2015 (Sector TIC): Marco regulatorio general de las Tecnologías de la Información y las Comunicaciones en Colombia.

Decreto 1008 de 2018: Establece los lineamientos generales de la Política de Gobierno Digital y su articulación con la estrategia del Estado. Guía No. 7 "Gestión de Riesgos" del Ministerio de las TIC: Orientaciones técnicas para la administración de riesgos tecnológicos.

Resolución 500 de 2021 del Ministerio de TIC que Define lineamientos e instrumentos institucionales para la transformación digital y la seguridad digital.

Resolución 02277 de 2025 del Ministerio de TIC que Actualiza formalmente el Modelo de Seguridad y Privacidad de la Información (MSPI) de las entidades públicas.

Norma Técnica Colombiana NTC-ISO/IEC 27001: Estándar internacional para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

5.4. Marco de Prevención de LA/FT/PADMCódigo Penal Colombiano

Ley 599 de 2000: Artículos 323 (delito de Lavado de Activos) y 345 (delito de Financiación del Terrorismo y administración de recursos relacionados). Directrices de la Unidad de Información y Análisis Financiero (UIAF): Estándares nacionales para la detección y el Reporte de Operaciones Sospechosas (ROS) aplicables como buena práctica corporativa.

5.5. Marcos de Emergencias, Riesgos Ambientales y Nuevas Tecnologías

Ley 1523 de 2012 (modificada por la Ley 2474 de 2025): Adopta la Política Nacional de Gestión del Riesgo de Desastres y regula el tratamiento preventivo de riesgos ambientales.

Acuerdo Distrital 003 de 2025: Marco normativo específico para el uso ético, seguro y transparente de Sistemas de Inteligencia Artificial en la administración pública, incluyendo auditorías algorítmicas.

4. ALCANCE

La presente política es aplicable a todo el direccionamiento estratégico de Canal Capital, a su estructura funcional y responsables de dependencias, procesos, programas, proyectos, planes, productos y servicios, así como a los bienes, recursos e instrumentos y la integridad con que son utilizados para el cumplimiento de la misión institucional.

Su alcance cobija la identificación, valoración, tratamiento, monitoreo, seguimiento y reporte de todas las tipologías de riesgos que se presenten en el marco de la gestión institucional. Bajo el enfoque del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), la entidad articula la mitigación de Riesgos Generales de la Gestión, Riesgos Fiscales y Riesgos de Seguridad de la Información con los riesgos para la integridad pública. Esta aproximación reconoce de forma transversal que un riesgo de gestión, fiscal o de seguridad de la información puede tener su causa originaria en un fallo de integridad —como el soborno, el fraude, la corrupción o un conflicto de intereses gestionado inadecuadamente—, o bien crear condiciones que favorezcan el lavado de activos, la financiación del terrorismo o la proliferación de armas de destrucción masiva (LA/FT/PADM). Por lo tanto, todas las tipologías descritas, incluyendo los riesgos ambientales y contractuales, se abordarán de forma integral y en estrecha articulación con la gestión institucional del riesgo y los lineamientos de la Política de Gobierno Digital.

Asimismo, esta política se extiende a las relaciones con contrapartes, contratistas, proveedores, aliados, convenios, asociaciones y demás terceros con los que Canal Capital interactúe en desarrollo de sus funciones, cuando dichas relaciones puedan impactar el logro de los objetivos institucionales o generar exposición a riesgos. Para el caso de los riesgos de seguridad digital y de la información, se aplicarán adicionalmente los lineamientos y criterios diferenciales definidos en los instrumentos institucionales y en la normativa vigente aplicable.

La presente política extiende su alcance a la transformación y fortalecimiento organizacional, tecnológica y de modelo de negocio en curso, reconociendo que la misión de Canal Capital se sustenta en su rol como medio de comunicación, canal público de televisión y empresa industrial y comercial del Estado, estableciendo la necesidad de identificar y tratar los riesgos derivados del uso de sistemas de Inteligencia Artificial (IA), algoritmos de aprendizaje automático y procesamiento de lenguaje natural aplicados en la producción de contenidos, interacción ciudadana y soporte administrativo, lo que incluye la gestión de riesgos asociados a los datos de entrenamiento para asegurar su calidad y evitar sesgos, la lógica algorítmica para garantizar la equidad y transparencia, y los resultados automatizados para evaluar su impacto en la toma de decisiones institucionales y en los derechos de los ciudadanos, entre otros.

5. COMPROMISO

Canal Capital se compromete a implementar, mantener y mejorar continuamente un sistema de gestión integral del riesgo, orientado a la creación, preservación y protección del valor público, que permita anticipar, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos que puedan afectar el cumplimiento de su misión, objetivos institucionales y la continuidad de su operación.

En coherencia con su rol como medio de comunicación público, canal público de televisión y Empresa Industrial y Comercial del Estado, y en el marco del Modelo Integrado de Planeación y Gestión (MIPG), Canal Capital asume el siguiente compromiso y establece los lineamientos operativos para la gestión integral del riesgo, reconociendo que su proactividad no es solo una obligación legal, sino un elemento constitutivo y estratégico de su estructura funcional, modelo de negocio e identidad. Dado que su principal activo es la credibilidad y su oferta central es

garantizar el derecho de acceso a la información pública —alineado con los Objetivos de Desarrollo Sostenible (ODS)—, el establecimiento de estas reglas, límites y lineamientos institucionales blinda la independencia editorial del canal, robustece su buen gobierno corporativo y asegura su rentabilidad social, transformando la transparencia en la mayor ventaja competitiva para la toma de decisiones y el fortalecimiento del negocio.

Por lo tanto, la administración general del riesgo en Canal Capital se hará bajo los siguientes lineamientos unificados:

1. Identificación y Administración Integral:

Identificar y administrar de manera integral todos los riesgos institucionales de gestión, integridad pública -incluyendo los relacionados con lavado de activos, financiación del terrorismo y proliferación de armas de destrucción masiva (LA/FT/PADM), fiscales, contractuales[2], ambientales, de seguridad y privacidad de la información, de acuerdo con su naturaleza y contexto. El alcance de esta política se extiende a la transformación tecnológica en curso, reconociendo la misión del canal como medio y canal público de televisión, estableciendo la necesidad de identificar y tratar los riesgos derivados del uso de sistemas de Inteligencia Artificial (IA), algoritmos de aprendizaje automático y procesamiento de lenguaje natural en la producción de contenidos, interacción ciudadana y soporte administrativo, lo que incluye la gestión de riesgos asociados a los datos de entrenamiento para asegurar su calidad y evitar sesgos, la lógica algorítmica para garantizar la equidad y transparencia, y los resultados automatizados para evaluar su impacto en la toma de decisiones institucionales y en los derechos de los ciudadanos.

2. Marco conceptual y Apetito de Riesgo:

Definir, aprobar y mantener actualizado el marco de apetito, tolerancia y capacidad de riesgo, como base para la toma de decisiones, la priorización de acciones y la evaluación de la aceptabilidad del riesgo, en coherencia con su direccionamiento estratégico, límites, reglas, lineamientos y procedimientos para el accionar.

3. Metodología Institucional Integrada:

Para su adecuada identificación, análisis, evaluación y tratamiento, la entidad cuenta con una metodología unificada del Departamento Administrativo de la Función Pública, los lineamientos distritales e internos que se expidan para su debida gestión, asegurando su integración con la planeación estratégica, la gestión por procesos y los instrumentos institucionales. Esta metodología es socializada y comunicada periódicamente a los líderes y responsables de los procesos institucionales. Los líderes de los procesos deben identificar los riesgos que puedan afectar el logro de los objetivos propuestos y determinar los controles que permitan disminuir su impacto y/o la probabilidad de ocurrencia.

[2] Los riesgos contractuales son abordados desde el proceso de contratación, de acuerdo con el Manual de Contratación vigente

4. Fortalecimiento del Modelo de Líneas de Defensa:

Fortalecer el modelo de líneas de defensa, asignando responsabilidades claras a la primera, segunda y tercera línea, para asegurar la gestión, supervisión y evaluación independiente del riesgo, promoviendo la rendición de cuentas.

5. Transparencia y Gestión de Riesgos de Integridad

Promover la gestión de riesgos de integridad pública, mediante la implementación de mecanismos preventivos, de detección y respuesta, en articulación con el Sistema Integrado de Gestión de Riesgos para la Integridad Pública (SIGRIP), los Programas de Transparencia y Ética Pública y la lucha contra la corrupción. Estos riesgos deben identificarse y revisarse periódicamente con el concurso de todas las dependencias y procesos, a fin de administrarlos, controlarlos y generar acciones preventivas que permitan minimizar o eliminar de forma estructural sus causas, sin perjuicio de las medidas que deban interponerse ante las autoridades competentes.

6. Gestión Diferenciada de Seguridad Digital y de la Información:

Gestionará de manera diferenciada los riesgos de seguridad digital y de la información, conforme a la normativa vigente, los lineamientos de Gobierno Digital vigentes, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los estándares aplicables. Tendrán manejo especial por parte del equipo de Gestión TIC, alineado con las guías y directrices emitidas por el Ministerio de TIC y los estándares internacionales adoptados, como los de seguridad de la información.

7. Prevención y Gestión de Riesgos LA/FT/PADM:

Implementará medidas para la prevención y gestión de riesgos LA/FT/PADM, mediante el fortalecimiento de controles, debida diligencia de contrapartes, monitoreo y capacitación continua, con el fin de salvaguardar la integridad institucional y su reputación, en cumplimiento de las directrices del DAFP y demás normativa vigente aplicable.

8. Formación, Monitoreo y Mejora Continua:

Promoverá la formación, sensibilización y comunicación permanente, asegurando que todos los servidores, contratistas y terceros comprendan sus responsabilidades frente a la gestión del riesgo. Asegurará el monitoreo, seguimiento y mejora continua, mediante el uso de indicadores clave de riesgo (KRI), evaluaciones periódicas y la incorporación de lecciones aprendidas.

9. Inteligencia Artificial (IA) Responsable y Sostenible:

Asegurar que cualquier implementación de la IA cumpla con los principios de transparencia, explicabilidad y supervisión humana (Human-in-the-loop), mitigando activamente sesgos algorítmicos. Proteger la integridad de los modelos de IA frente a ataques, contaminación de datos o fugas de información, en concordancia con la Política de Gobierno Digital vigente y el Acuerdo aplicable. Establecer mecanismos de rendición de cuentas sobre los impactos sociales y éticos de los sistemas automatizados utilizados por la entidad.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

10. Implementación y prospectiva

La presente política será revisada y actualizada como mínimo cada veinticuatro (24) meses, o cuando se presenten cambios normativos u organizacionales. Esta revisión estará a cargo de la Alta Dirección, con el soporte de la segunda línea de defensa, y será validada en las instancias institucionales correspondientes. La versión vigente será publicada en los medios institucionales definidos y constituirá la única versión oficial y controlada.

Este compromiso se materializa a través de tres dimensiones internas:

- Una cultura organizacional basada en la capacitación continua para que todos los colaboradores identifiquen y reporten situaciones riesgosas.
- La armonización con el Sistema de Gestión Integral de Riesgos y el Programa de Transparencia y Ética Pública.
- La implementación de mecanismos de debida diligencia y canales institucionales para la denuncia de operaciones sospechosas que no resulten razonables frente a una actividad económica determinada.

11. Procesos y áreas con mayor exposición al riesgo

Las áreas y procesos con exposición a riesgos de LA/FT/PADM deben detectar comportamientos atípicos analizando información de clientes, proveedores y Personas Expuestas Políticamente (PEP). Se consideran criterios orientadores o señales de alerta situaciones como:

- Operaciones con clientes de derecho privado que superen los **10 SMMLV**.
- Pagos provenientes de cuentas de terceros u ofrecimientos de pagos en efectivo.
- Anticipos injustificados o gastos significativamente superiores al promedio del mercado sin soporte técnico.
- Cualquier evento que pueda asociarse razonablemente a prácticas de corrupción o factores de riesgo.
- Estar incluido en la lista de proveedores ficticios de la DIAN.
- Hallazgos de información falsa de la contraparte, entre otros.

Una vez detectada una operación inusual, la **segunda línea de defensa** realizará un análisis basado en criterios objetivos sobre su relevancia y complejidad, asegurando que las conclusiones sean de conocimiento del Órgano de cumplimiento normativo.

Si se configura una **Operación Sospechosa**, se recomendará a la línea estratégica realizar el **Reporte de Operación Sospechosa (ROS)** ante la Unidad de Información y Análisis Financiero (UIAF) a través del enlace institucional "Informe sobre temas de LA/FT". Este procedimiento es igualmente aplicable a denuncias de anticorrupción y atención al ciudadano vinculadas a estos delitos.

Aunque Canal Capital no se encuentra registrado en la plataforma SIREL[3] de la UIAF, adopta por buena práctica la elaboración de reportes a este sistema[4] que deben contener como mínimo:

1. Descripción detallada de la operación y periodo de tiempo.
2. Identificación plena de las personas naturales o jurídicas involucradas.
3. Señales de alerta detectadas con sus respectivos soportes documentales y anexos que evidencien los cambios de comportamiento.

El reporte oportuno de estos eventos a través de las líneas de defensa permite orientar la gestión institucional y, de ser procedente, informar a las autoridades competentes.

6. ROLES Y RESPONSABILIDADES

Línea de defensa	Responsable	Responsabilidad
Línea estratégica	Alta Dirección	● Definir, aprobar y revisar la política de gestión integral del riesgo; establecer el apetito, tolerancia y capacidad de riesgo de la entidad; fijar los límites de exposición aceptables; asegurar la integración de la gestión del riesgo con la estrategia institucional, MIPG, SIGRIP y demás instrumentos de gestión; promover el "tono desde la cima" y asignar recursos para la gestión del riesgo. ● Evaluar el estado del sistema, acorde con la información generada por parte de 2da línea identificadas y la actividad de control definida que materializa las líneas de reporte en cada caso, de acuerdo con el tema que son responsables, a fin de generar acciones y una toma de decisiones con enfoque preventivo.
	Comité Institucional de Coordinación de Control Interno – CICCI	● Recomendar ajustes y aprobar la política y los criterios de gestión del riesgo; conocer el estado de la gestión del riesgo a partir de los informes de primera y segunda línea; hacer seguimiento al sistema de control interno y a la efectividad de la gestión del riesgo; orientar acciones de fortalecimiento y mejora. ● Emitir recomendaciones respecto al cumplimiento y la adaptación de los aspectos en materia de riesgos como parte integral de la administración de este al interior de la entidad. ● Monitorear la efectividad de la gestión del riesgo en el marco del CICCI, tomando como base los informes generados de la primera y segunda línea.

[3] Función: Herramienta web para que los sujetos obligados carguen, reporten y revisen información de operaciones sospechosas (ROS).

[4] La práctica estándar global es que los ROS se hacen ante las *UIF*. En Colombia la autoridad es la UIAF, única entidad a cargo de la plataforma de reportes de este tipo denominada SIREL.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

Línea de defensa	Responsable	Responsabilidad
	Comité Institucional de Gestión y Desempeño - CIGD	● Recomendar ajustes a la política y los criterios de gestión del riesgo; conocer el estado de la gestión del riesgo a partir de los informes de segunda línea ● Analizar periódicamente los resultados del monitoreo de riesgos institucionales; revisar la articulación entre la gestión del riesgo, el direccionamiento estratégico y los demás instrumentos institucionales; promover mejoras en los procesos, controles e instrumentos de gestión.
Primera línea	Líderes y responsables de procesos	● Identificar, valorar, tratar y monitorear los riesgos de sus procesos, programas, proyectos y planes; ejecutar y evidenciar los controles; reportar eventos materializados; adelantar autoevaluaciones; mantener trazabilidad de la gestión del riesgo; socializar la política y metodología con sus equipos; aplicar acciones correctivas y de mejora. ● Certificar mediante comunicación formal, o correo electrónico o a través de los sistemas de información disponibles, periódicamente la existencia o no de eventos de riesgo en sus procesos, como mínimo cuando se realice un monitoreo o seguimiento desde segunda línea, garantizando la veracidad, oportunidad y completitud de la información reportada. ● Analizar y hacer seguimiento a los riesgos y efectuar controles para mitigar la materialización, de conformidad con lo establecido en la presente política, reportar a la segunda línea y proponer mejoras a la gestión del riesgo en su proceso. ● Adelantar actividades de autoevaluación para determinar la eficiencia, eficacia y efectividad de los controles de manera periódica. ● Informar a la segunda y tercera línea aquellos riesgos materializados en las actividades a su cargo y adelantar las gestiones competentes según aplique (tener en cuenta lo establecido en el numeral 10 de la presente política). ● Llevar trazabilidad y mantener para consulta las evidencias de la gestión de los riesgos a su cargo. ● Socializar y fomentar de forma continua al interior de sus equipos de trabajo los temas relacionados con la gestión del riesgo del proceso correspondiente. ● Asegurar que al interior de su grupo de trabajo se reconozca el concepto de administración del riesgo, la política y la metodología definida para administrar el riesgo, aprobados por la línea estratégica. ● El Oficial de Seguridad de la Información verifica el desarrollo y mantenimiento de los controles de Tecnologías de la Información identificados. ● Respecto a riesgos de integridad, es necesario hacer la identificación y recopilación de información de los clientes y proveedores que intervienen en la operación de los procesos de contratación, teniendo en cuenta aquellos susceptibles de involucrarse en riesgos asociados con actividades ilícitas. ● Desarrollar habilidades y competencias para identificar riesgos de alucinaciones, sesgos de género/raza o errores técnicos en los resultados de la IA.

Línea de defensa	Responsable	Responsabilidad
Segunda línea	Oficina Asesora de Planeación Gestión TIC Supervisores Responsables de sistemas de gestión y políticas del MIPG Órgano de Cumplimiento	● Asesorar a la Alta Dirección en la actualización de la Política; proponer criterios de impacto, tolerancia y aceptación del riesgo; consolidar y socializar las matrices institucionales; orientar metodológicamente a la primera línea; validar que los controles sean pertinentes y estén diseñados y ejecutados conforme a su propósito; monitorear KRI y alertas tempranas; promover la capacitación y la mejora continua; asegurar la articulación con SIGRIP, MIPG y demás instrumentos. ● Consolidar las matrices de riesgos institucionales y socializarlas en el Comité de Gestión y Desempeño Institucional para su análisis y seguimiento. ● Recibir reportes o informes sobre materialización de riesgos u operaciones inusuales y emitir recomendaciones sobre los controles implementados por la primera línea de defensa. ● Informar al Órgano de cumplimiento cuando la materialización de un riesgo haya implicado operaciones inusuales o actuaciones demostrables de colaboradores que permitan inferir un delito fuente con riesgo atinente a LA/FT/PADM. ● Acompañar, orientar y sensibilizar a los líderes de proceso y responsables de primera línea en la identificación, análisis y valoración del riesgo en todas las tipologías. ● Promover actividades de autoevaluación para determinar la eficiencia, eficacia y efectividad de los controles. ● Verificar que el diseño de los controles establecidos por la primera línea sea pertinente frente a los riesgos identificados en cuanto a responsables, propósito, periodicidad, tratamiento, evidencias de ejecución, así como verificar que se estén ejecutando según fueron diseñados y adelantar las recomendaciones pertinentes. ● Monitorear periódicamente la gestión y tratamiento dado a los riesgos desde la primera línea. ● Promover la capacitación e inducción y generar recomendaciones relacionadas con la gestión del riesgo. ● Definir la metodología para la Administración o gestión del Riesgo. ● Socializar al interior de la entidad los instrumentos de administración del riesgo, aprobados por la línea estratégica. ● Fomentar que la gestión para todas las operaciones cumpla con las leyes y regulaciones aplicables en materia de *LA/FT/PADM*. ● Realizar seguimiento a la implementación de las medidas correctivas que haya implicado la materialización de uno o más riesgos

Línea de defensa	Responsable	Responsabilidad
Tercera línea	Oficina de control interno	● Realizar actividades de evaluación objetiva de la efectividad de la gestión del riesgo, plasmados en el mapa de aseguramiento de Capital. ● Evaluar la efectividad de los controles de segunda línea, plasmados en el mapa de aseguramiento de Capital. ● Evaluar la efectividad de los controles de primera línea, que no se encuentren cubiertos por la segunda línea, plasmados en el mapa de aseguramiento de Capital. ● Adelanta los ejercicios de revisión, actualización y evaluación de la confianza del mapa de aseguramiento. ● Alertar sobre riesgos no identificados o controles insuficientes de conformidad con los lineamientos definidos por la alta dirección. ● Adelantar el seguimiento a los mapas riesgos [evaluando la efectividad de las acciones desarrolladas] de conformidad con la programación establecida en el Plan Anual de Auditorías y socializar los resultados a los líderes de proceso y en el marco del Comité Institucional de Coordinación de Control Interno. ● Recomendar mejoras a la política de administración de riesgo. ● Verificar la implementación de las medidas correctivas que haya implicado la materialización de uno o más riesgos

7. GUÍAS DE ACCIÓN, DISEÑO Y PLANEACIÓN

Canal Capital adopta los siguientes niveles de severidad del riesgo, producto del cruce entre los grados de probabilidad e impacto, con el fin de establecer las escalas para su tratamiento e implementarlas en las diferentes matrices de riesgos. La Alta Dirección definirá y aprobará los niveles de apetito de riesgo para cada tipología (gestión, integridad, seguridad digital y fiscal), estableciendo las desviaciones máximas permitidas (tolerancia) y los límites de capacidad institucional frente a escenarios críticos

9.1. Niveles de severidad del riesgo

La Entidad adopta una escala de severidad para clasificar, priorizar y tratar los riesgos, en estricto cumplimiento de la metodología institucional y los lineamientos de la Guía de Gestión Integral del Riesgo V7. Este marco se complementa con la definición de umbrales cuantitativos y cualitativos de apetito, tolerancia y capacidad, los cuales se alinean con los objetivos estratégicos, procesos misionales e indicadores de desempeño para identificar desviaciones que requieran intervención.

Para garantizar un monitoreo preventivo, se incorporan Indicadores Clave de Riesgo (KRI) e Indicadores Clave de Proceso (KPI). Estos instrumentos activan una alerta temprana para detectar aproximaciones o desviaciones de los límites definidos y fundamentar la toma de decisiones sobre el tratamiento institucional.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

Las acciones de aceptación, evitación, reducción o transferencia se determinarán según la zona de severidad y el nivel de tolerancia aprobado:

- Gestión Operativa: Los riesgos que se mantengan dentro del apetito definido podrán ser aceptados directamente por el responsable del proceso.

- Escalamiento: Aquellos que superen los límites establecidos deberán remitirse a la instancia competente. Los riesgos de severidad alta o extrema requerirán, sin excepción, la evaluación y aprobación expresa de la Alta Dirección o su delegado.

Finalmente, cualquier ajuste a la severidad o decisión de tratamiento deberá sustentarse en un análisis técnico integral que evidencien la efectividad de los controles, la valoración del riesgo residual y su coherencia con el apetito de riesgo institucional.

El mapa de calor en imagen permite visualizar la exposición de los riesgos a partir de la combinación de su probabilidad e impacto. Los criterios y la metodología detallada para la aplicación de este instrumento y la definición del apetito de riesgo institucional se desarrollan en el Manual Metodológico para la Administración del Riesgo EPLE-MN-003. MANUAL METODOLÓGICO PARA LA ADMINISTRACIÓN DEL RIESGO.

PROBABILIDAD >				
	5-Muy alta (100%)	15	20	25
	4-Alta (80%)	12	16	20
	3-Media (60%)	9	12	15
	2-Baja (40%)	6	8	10
	1-Muy baja (20%)	3	4	5
		3-Moderado (60%)	4-Mayor (80%)	5-Catastrófico (100%)
	IMPACTO >			

Moderado
Alto
Extremo

9.2. Tratamiento del riesgo

TIPO DE RIESGO	ZONA DE RIESGO	OPCIONES DE TRATAMIENTO DEL RIESGO
Riesgos de Gestión	Baja	**Asumir el riesgo.** Se administra a través de las actividades del proceso, proyecto o plan. Se debe adelantar un monitoreo *semestralmente* por parte de los líderes de proceso con el fin de verificar que estos riesgos no surten cambios en su aceptación que requiera la implementación de actividades de control. El reporte de su gestión se registrará en la herramienta determinada por el proceso [Acta de reunión, correo, reporte a OAP u otro].
	Moderada	**Reducir el riesgo.** Implementación de acciones de control preventivas que permitan reducir la probabilidad. Su monitoreo se realizará *semestralmente* por los líderes de proceso y sus equipos de trabajo con el fin de verificar que estas mitigan la materialización del riesgo identificado, se registrará en la herramienta determinada por el proceso [Acta de reunión, correo, reporte a OAP u otro].
	Alta y Extrema	Manejo a través del mapa de riesgos del proceso e institucional, estableciendo acciones preventivas. Su monitoreo se realizará *trimestralmente* por parte de los líderes de proceso y la ejecución de esta actividad se registrará en la herramienta determinada por el proceso [Acta de reunión, correo, reporte a OAP u otro].
Riesgos de Integridad Pública y *LA/FT/PADM*	Moderada	**Reducir el riesgo** Implementación de acciones de control preventivas que permitan reducir la probabilidad. Su seguimiento se realizará *semestralmente* por parte de los líderes de proceso y la ejecución de esta actividad se registrará en la herramienta determinada por el proceso [Acta de reunión, correo, reporte a OAP u otro].
	Alta y Extrema	**Reducir, evitar y transferir o compartir el riesgo** • **Reducir:** disminuir la probabilidad o impacto, o ambos. Implementación de controles. • **Evitar:** impedir su materialización. No con la actividad que causa el riesgo. • **Transferir o compartir:** reducir el efecto del riesgo a través del traspaso de parte de las pérdidas a otro actor. Su seguimiento se realizará de forma trimestral por parte de los líderes de proceso y la ejecución de esta actividad se registrará en la herramienta determinada por el proceso [Acta de reunión, correo, reporte a OAP u otro].

En función de la zona de riesgos se deben establecer lineamientos que permitan la administración de estos y la toma de decisiones sobre los mismos, considerando las siguientes opciones:

○ **Aceptar o asumir el riesgo:** si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo. La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el

riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

- **Evitar el riesgo:**[5] Cuando los escenarios de riesgos identificados se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

- **Compartir o transferir el riesgo**[6]**Cuando** es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

- **Reducir el riesgo**[7]**:** El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Nota: Ningún riesgo asociado a la toma de decisiones automatizadas que impacte derechos fundamentales o recursos públicos podrá ser clasificado en zona Baja. Se prohíbe la 'Aceptación del Riesgo' (Asumir) en sistemas de IA que carezcan de supervisión humana directa.[8]

10. MANEJO DE RIESGOS MATERIALIZADOS

10.1. Gestión de eventos materializados

Con el propósito de fortalecer la gestión integral del riesgo y garantizar la oportuna identificación, tratamiento y aprendizaje institucional frente a la materialización de eventos de riesgo se deberá garantizar que todos los eventos de riesgo materializados sean reportados y gestionados de manera estructurada, oportuna y trazable, en alineación con los lineamientos del SIGRIP y el Sistema de Control Interno, asegurando su adecuada detección, contención, análisis, reporte y mejora continua. Para tal efecto, se establecen las siguientes directrices:

10.1.1. Obligatoriedad del reporte periódico

Con periodicidad trimestral, todas las áreas deberán presentar el reporte formal sobre el estado

[5] Ibid., Pág. 71

[6] Ibid., Pág. 72

[7] Ibid., Pág. 72

[8] Acuerdo No. 003 de 2025 - Consejería TIC

de sus riesgos. Este informe incluirá, de manera obligatoria, la certificación expresa sobre la ocurrencia o ausencia de eventos materializados durante el periodo, garantizando así la trazabilidad y el fortalecimiento del control institucional. Esta certificación se formaliza de acuerdo con el Manual de Gestión del Riesgo.

10.1.2. Reporte inmediato de eventos de riesgo

Ante la identificación de un evento de riesgo, el líder del proceso o cualquier integrante del área, debe reportarlo inmediatamente a la Oficina Asesora de Planeación bajo el procedimiento definido en el manual de riesgos y a las instancias de segunda y tercera línea establecidas en esta Política. Este reporte se realizará de manera independiente a los informes periódicos, proporcionando los datos necesarios para su análisis técnico por parte de la Oficina Asesora de Planeación.

10.2. Procedimiento

El procedimiento de gestión de eventos de riesgo deberá activarse ante la ocurrencia o identificación de cualquier evento que genere o pueda generar afectaciones operativas, financieras, legales o reputacionales. La activación deberá basarse en criterios previamente definidos, tales como tipología del riesgo, nivel de impacto y recurrencia del evento.

10.2.1 Etapas Mínimas del Proceso

Todo evento materializado deberá ser gestionado como mínimo a través de las siguientes etapas:

10.2.1.1 Detección: Identificación oportuna del evento por parte del responsable del proceso o cualquier colaborador.

10.2.1.2 Contención: Implementación inmediata de acciones orientadas a mitigar el impacto y evitar su propagación.

10.2.1.3. Investigación interna: Análisis de causas raíz, incluyendo factores internos y externos asociados al evento.

10.2.1.4. Reporte: Notificación formal al Órgano de Cumplimiento, Segunda Línea y Control Interno mediante correo electrónico o memorando y, cuando corresponda, a las autoridades competentes mediante oficio.

10.2.1.5. Cierre y lecciones aprendidas: Documentación de conclusiones y presentación en CIGD, definición de acciones correctivas y preventivas, y socialización de aprendizajes mediante el formulario de Lecciones Aprendidas y Buenas Prácticas EPLE-FT-040.

10.2.2. Asignación de Responsabilidades

El CIGD debe definir y formalizar los roles y responsabilidades para cada etapa del proceso, garantizando como mínimo:

- Responsables de detección y contención en cada proceso. (Primera línea)
- Responsables de investigación (Control Interno, Control Interno Disciplinario y/o Órgano de Cumplimiento).
- Responsables de reporte (Segunda línea y Tercera Línea)

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

- Instancias de revisión y aprobación (Comités o Alta Dirección).

10.2.3. Registro y Trazabilidad

Todos los eventos materializados deberán ser registrados en los sistemas o herramientas definidas por la Entidad según su Manual de Gestión del Riesgo (matriz de riesgos, sistemas de incidentes o equivalentes), garantizando:

- Identificación única del evento.
- Registro de fechas, responsables y actuaciones.
- Soporte documental y evidencias.
- Seguimiento hasta su cierre.

10.2.4. Clasificación del evento

Cada evento deberá ser clasificado de acuerdo con su naturaleza y con la tipología de riesgo que corresponda, conforme a las categorías y definiciones establecidas en el glosario institucional, así como con su nivel de impacto (alto, medio o bajo), con el fin de priorizar su gestión y definir los niveles de escalamiento correspondientes.

10.2.5. Tiempos de gestión

El EPLE-MN-003. MANUAL METODOLÓGICO PARA LA ADMINISTRACIÓN DEL RIESGO establecerá los plazos máximos para cada etapa del proceso, incluyendo detección, contención, investigación y cierre del evento, así como indicadores de seguimiento que permitan evaluar la oportunidad y efectividad de la gestión.

10.2.6. Escalamiento

El EPLE-MN-003. MANUAL METODOLÓGICO PARA LA ADMINISTRACIÓN DEL RIESGO establecerá criterios claros de escalamiento para eventos de alto impacto o criticidad, incluyendo la obligación de informar a la Alta Dirección, Comités institucionales y autoridades externas, cuando aplique.

10.2.7. Articulación con la gestión de riesgos

Como resultado de la materialización de eventos, la Entidad deberá actualizar la matriz de riesgos correspondiente hasta máximo en dos periodos de actualización a la gestión del riesgo, según cronograma de Segunda Línea, revisando la valoración del riesgo (inherente y residual), incorporando nuevas causas y fortaleciendo los controles existentes.

10.2.8. Seguimiento y control

La segunda línea adelanta el monitoreo a la implementación a las acciones y la tercera adelanta el seguimiento y evaluación a la efectividad de las acciones preventivas y correctivas definidas, así como a la posible reincidencia de eventos similares, en el marco de los procesos de auditoría interna y control institucional.

10.2.9. Comunicación y confidencialidad

La gestión de eventos materializados deberá realizarse por medio de correo electrónico o memorando al supervisor o Líder del proceso, así como la segunda y tercera línea de defensa, garantizando la confidencialidad de la información y el adecuado manejo de datos sensibles para la empresa o los servidores.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

10.3. Acciones específicas por tipología de riesgo

10.3.1. Riesgos de Integridad[9, 10]

La gestión de riesgos materializados asociados a soborno, fraude, corrupción o conflicto de intereses gestionado inadecuadamente se realizará bajo el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), en el marco de los Programas de Transparencia y Ética Pública. De este modo se adopta para fines de esta Política y documentos asociados, el concepto de integridad, que además de medidas contra la corrupción contempla una integralidad de acciones de control que reconocen los diferentes fenómenos que atentan contra la integridad.

En el evento de materializarse un **riesgo de integridad**, es necesario realizar los ajustes con acciones, tales como:

LÍNEA DE DEFENSA	RESPONSABLE	ACCIÓN
Primera línea	Áreas y procesos que identifican la materialización del riesgo dentro de la gestión	Informar a la Oficina de Control Interno y a la Oficina Asesora de Planeación sobre la situación presentada con el fin de adelantar las investigaciones del caso.
Segunda línea	Oficina Asesora de Planeación Órgano de Cumplimiento El líder de área o supervisor que por su competencia, procedimientos a cargo y responsabilidades de segunda línea de defensa tengan conocimiento del riesgo de integridad reportado. Control Interno Disciplinario	Abrir espacios con los responsables del proceso afectado con la finalidad de analizar la información documentada en la matriz de riesgos y adelantar los ajustes correspondientes, informar al Órgano de cumplimiento cuando el riesgo pueda implicar actuaciones demostrables de colaboradores que permitan inferir un delito contra la integridad, así como presentar las novedades ante el CIGD en el marco de los monitoreos periódicos realizados a los riesgos. Llevar a cabo la revisión de los controles y acciones del plan de manejo de riesgos teniendo en cuenta las características de la materialización y los puntos importantes de la gestión Adelantar las investigaciones según

[9] Ibid., Pág. 74

[10] Frente a la materialización de un riesgo de integridad pública o de conductas que puedan constituir faltas disciplinarias o delitos contra la administración pública, cualquier servidor público o contratista que lo detecte tiene el deber legal de reportarlo a la Oficina de Control Disciplinario Interno y/o interponer la respectiva denuncia ante las autoridades competentes (Fiscalía General de la Nación, Procuraduría General de la Nación o Personería de Bogotá), sin necesidad de agotar trámites previos o validaciones en las líneas de defensa. Lo anterior, sin perjuicio de que la primera y segunda línea activen de forma paralela los protocolos internos de contención operativa del riesgo y actualización del mapa de riesgos institucional.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

		corresponda, así como trasladar por competencia a los entes de control.
Tercera línea de defensa[11]	Control Interno	Informar la situación reportada en el CICCI Recomendar mejoras para la valoración de los riesgos y la documentación de controles Adelantar las investigaciones según corresponda Retroalimentar al sistema de cumplimiento sobre debilidades en los riesgos
Línea Estratégica	Alta Dirección Junta Administradora Regional	Coordinar el reporte adecuado a las autoridades competentes, cumpliendo con los requisitos regulatorios. Fortalecer la capacitación y concientización del personal sobre los riesgos y controles en materia de Integridad Evaluar la efectividad de la actuación frente a los riesgos materializados, conforme a lo establecido en la presente política.

10.3.2. Riesgos relacionados con lavado de activos y financiación del terrorismo - LA/FT/FPADM:

En el evento de materializarse un riesgo de LA/FT/FPADM, es necesario realizar acciones tales como:

LÍNEA DE DEFENSA	RESPONSABLE	ACCIÓN
Primera línea	Áreas y procesos que identifican la materialización del riesgo dentro de la gestión	Suspender preventivamente cualquier trámite asociado a la transacción o contraparte sospechosa. Informar inmediatamente a la Oficina Asesora de Planeación y al Órgano de Cumplimiento (segunda

[11] La Oficina de Control Interno debe asegurar que los controles sean efectivos y le apunten a mitigar la materialización del riesgo, así como que estén funcionando en forma oportuna y efectiva, Mientras que Control Disciplinario Interno, según corresponda adelanta las investigaciones de carácter disciplinario que comprometan la integridad de los servidores públicos.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

		línea). Informar a la Subdirección Financiera para realizar la trazabilidad y/o bloqueo preventivo en las cuentas o registros de tesorería. Recopilar de forma segura todos los soportes documentales y evidencias de la operación atípica detectada.
Segunda línea	Órgano de Cumplimiento Oficina Asesora de Planeación Subdirección Financiera	Realizar el análisis técnico objetivo de la operación sospechosa detectada. En caso de configurarse formalmente una operación sospechosa, estructurar y tramitar el **Reporte de Operación Sospechosa (ROS) ante la UIAF**. (SF) Convocar a mesas de trabajo técnicas para revisar los controles de debida diligencia de la contraparte y actualizar el mapa de riesgos correspondiente.
Tercera línea de defensa	Oficina de Control Interno	Evaluar de manera independiente la oportunidad del reporte del ROS ante la UIAF y el cumplimiento de los tiempos de escalamiento. Recomendar mejoras estructurales para mitigar vulnerabilidades en el diseño de los controles de prevención del lavado de activos y financiación del terrorismo.
Línea Estratégica	Alta Dirección Junta Administradora Regional	Respaldar institucionalmente el envío de reportes confidenciales a la UIAF y coordinar la comunicación oficial con la Fiscalía General de la Nación u otros entes penales si corresponde. - Asignar los recursos y herramientas tecnológicas especializadas para robustecer los procesos de debida diligencia de proveedores y clientes. - Aprobar el plan de capacitación obligatorio y especializado en prevención de LA/FT/PADM para todo el personal.

10.3.3. Riesgos de gestión, ambientales y de seguridad digital

Líder de Proceso

Para riesgos ubicados en **zona de riesgo extrema y alta**

✓ Informar a la OCI y a la OAP sobre la situación presentada con el fin de adelantar las investigaciones del caso.

✓ Identificar las acciones que puedan implementarse y revisar los riesgos del proceso – Actualizar el mapa de riesgos.

✓ Informar a la Oficina Asesora de Planeación cuando son materializaciones de los riesgos de proceso y proyecto, a sistemas cuando son riesgos de seguridad digital y a la Subdirección Administrativa para el caso de los riesgos ambientales.

Para los riesgos ubicados en **zona de riesgo moderada y baja**

✓ Establecer las acciones correctivas a que haya lugar.

✓ Informar a la Oficina Asesora de Planeación los riesgos de gestión, y proyectos, a sistemas los riesgos de seguridad digital y a la Subdirección Administrativa los riesgos ambientales.

✓ Verificar la calificación del riesgo y su ubicación en el mapa de riesgos.

Oficina de Control Interno

- Evalúa y comunica al responsable la situación detectada, con copia a la Oficina Asesora de Planeación (cuando se trate de riesgos de proceso, proyectos -gestión, integridad-), a la Subdirección Administrativa (Líder proceso ambiental) cuando se identifiquen causas potenciales de riesgos ambientales y al área de Tecnologías de la Información y Comunicaciones (cuando se identifique materialización de riesgos de seguridad digital), con el fin de contar con el asesoramiento correspondiente y aplicar las medidas correctivas (cuando haya lugar a ello).
- Emite alertas tempranas al responsable del activo de información, proceso o proyecto en el establecimiento de acciones correctivas y de mejora.
- Evalúa la efectividad de las acciones propuestas por el responsable del activo de información, proceso o proyecto con la periodicidad determinada en el Plan Anual de Auditoría.
- Informa los hallazgos y proporciona recomendaciones de forma independiente.
- Evalúa la efectividad de los controles definidos para mitigar los riesgos identificados

10.4. Actividades para la identificación y la gestión de riesgos desde la primera línea

La gestión de riesgos en Canal Capital sigue un ciclo lógico y continúo enfocado en la prevención y la mejora constante. Las actividades a cargo de los líderes y referentes de proceso se ejecutan bajo la siguiente secuencia metodológica:

10.4.1. Identificación, Análisis y Evaluación (Planear / Diseñar)

En esta fase inicial, cada proceso debe mapear sus vulnerabilidades y diseñar la estrategia de mitigación de forma proactiva.

Identificación y Documentación: El líder del proceso, con el apoyo de su "Referente de Proceso", registrará los riesgos y sus causas en la matriz de riesgos institucional, según las directrices metodológicas vigentes.

Diseño de Controles: Se diseñarán controles proporcionales con base en la escala de severidad y el apetito de riesgo aprobado.

Socialización Obligatoria: El referente de proceso comunicará los riesgos identificados, controles y tratamiento al interior del equipo de trabajo y a los grupos de valor.

10.4.2. Monitoreo y Ejecución de Controles (Hacer / Implementar)

Consiste en la aplicación diaria de las actividades de control y el autoregistro de su efectividad.

Ejecución de Controles: La Primera Línea ejecuta y recopila evidencias diarias/periódicas del funcionamiento de los controles.

Registro de Avances: El referente de proceso consolida de manera constante los soportes del monitoreo para reportar el estado de los controles a la Segunda Línea.

10.4.3. Períodos de Revisión y Mesa de Trabajo (Verificar / Evaluar)

Para asegurar que los mapas de riesgo no pierdan vigencia frente a los cambios institucionales, se establecen los siguientes plazos de revisión periódica obligatoria:

Riesgos de Gestión, Ambientales y de Seguridad Digital: Validación y actualización obligatoria como mínimo una (1) vez al año (por vigencia mediante mesas de trabajo internas lideradas por el proceso y acompañadas por la Oficina Asesora de Planeación o según se identifique necesidad de revisión a partir de monitoreo o eventos materializados.

Riesgos de integridad pública incluyendo LA/FT/PADM: Debido a su criticidad, su identificación y validación se realizará obligatoriamente de manera semestral.

Autoevaluación de Procesos: Los líderes realizarán un ejercicio de autoevaluación integral de la efectividad de sus controles como mínimo una (1) vez al año, mediante el instrumento dispuesto en el SIG

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

10.4.4. Monitoreo de Segunda Línea y Seguimiento de Tercera Línea (Aseguramiento)

Segunda Línea de Defensa: La Oficina Asesora de Planeación (OAP) adelantará dos (2) actividades de monitoreo anuales estructuradas para validar el diseño y ejecución de los controles.

Tercera Línea de Defensa: La Oficina de Control Interno evaluará la efectividad real y el cumplimiento de las acciones de tratamiento de acuerdo con el Plan Anual de Auditoría.

10.4.5. Gestión ante la Materialización de Riesgos (Actuar / Ajustar)

Si un evento de riesgo llega a ocurrir a pesar de los controles, se activará inmediatamente el protocolo definido en el numeral 9.2 (Detección→ Contención→ Investigación→ Reporte Lecciones Aprendidas).

Como acción de cierre obligatorio ante una materialización, el proceso tendrá un plazo máximo el siguiente periodo de actualización programados en el Cronograma de segunda línea, para reestructurar y robustecer sus controles en la matriz de riesgos.

11. MONITOREO, EVALUACIÓN Y SEGUIMIENTO DE LA GESTIÓN DE RIESGOS

La gestión de riesgos se desarrolla bajo un esquema de líneas de defensa, en el cual cada línea tiene responsabilidades diferenciadas. La primera línea gestiona directamente los riesgos y ejecuta los controles; la segunda línea realiza el monitoreo y acompañamiento metodológico; y la tercera línea efectúa la evaluación independiente.

11.1. Gestión y autocontrol – Primera Línea de Defensa

Los líderes y responsables de los procesos deberán gestionar los riesgos asociados a sus objetivos y actividades, ejecutar los controles establecidos, realizar el autocontrol y reportar oportunamente las desviaciones, materializaciones de riesgos o situaciones que puedan afectar el cumplimiento de los objetivos institucionales.

11.2. Monitoreo – Segunda Línea de Defensa

La segunda línea de defensa, a cargo de la Oficina Asesora de Planeación o quien haga sus veces, realizará el monitoreo de la gestión de riesgos mediante actividades de orientación, acompañamiento y verificación, entre ellas:

- Verificar la aplicación de la metodología institucional para la gestión de riesgos.
- Acompañar a los procesos en la identificación, valoración, tratamiento y actualización de

los riesgos.
- Analizar y consolidar la información reportada por los procesos.
- Verificar el avance en la ejecución de los controles y las acciones de tratamiento.
- Identificar alertas, desviaciones y oportunidades de mejora.
- Informar los resultados del monitoreo a las instancias correspondientes.

Nota: El monitoreo realizado por la segunda línea no reemplaza la responsabilidad de los líderes de proceso sobre la gestión de sus propios riesgos ni constituye una evaluación independiente.

11.3. Evaluación independiente – Tercera Línea de Defensa

La tercera línea de defensa, a cargo de la Oficina de Control Interno, realizará la evaluación independiente de la gestión de riesgos y de la efectividad de los controles, de acuerdo con sus competencias legales y reglamentarias.

Esta evaluación podrá incluir la revisión de:

- La aplicación de las políticas, metodologías y procedimientos relacionados con la gestión de riesgos.
- La efectividad de los controles establecidos.
- La gestión realizada por los procesos frente a los riesgos identificados.
- La implementación de acciones de mejora derivadas de evaluaciones, auditorías o seguimientos.

Los resultados de las evaluaciones independientes y las recomendaciones correspondientes serán comunicados a las instancias competentes para la toma de decisiones y el fortalecimiento de la gestión institucional.

12. FUENTES Y BIBLIOGRAFÍA

- Departamento Administrativo de la Función Pública – DAFP. *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas*. Versión vigente. Fuente: Departamento Administrativo de la Función Pública – DAFP

- Departamento Administrativo de la Función Pública – DAFP. *Modelo Integrado de Planeación y Gestión – MIPG*. Fuente: Modelo Integrado de Planeación y Gestión – MIPG

- Organización Internacional de Normalización – ISO. *ISO 31000:2018 – Risk management — Guidelines*. Fuente: ISO 31000:2018 – Risk management

- Committee of Sponsoring Organizations of the Treadway Commission – COSO. *Enterprise Risk Management – Integrating with Strategy and Performance*. 2017. Fuente: COSO Enterprise Risk Management

- Alcaldía Mayor de Bogotá D.C. / Secretaría General. Lineamientos y documentos relacionados con el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP. Fuente: Alcaldía Mayor de Bogotá D.C.

- Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. Lineamientos y documentos relacionados con la gestión de riesgos de seguridad digital y de la información.
  Fuente: Ministerio TIC