Política de Gestión Integral de Riesgo

DS
DISTRISEGURIDAD

2026

Política de Gestión Integral de Riesgo- Distriseguridad

Código	*POL – DEYP - 001*
Versión	*2.0*
Fecha	*Marzo de 2026*
Dependencia líder	*Direccionamiento Estratégico y Planeación*
Aprobación	*Comité de Coordinación de Control Interno*

CONTROL DE CAMBIOS

Este control de cambios registra de forma resumida las versiones y modificaciones relevantes del documento.

Versión	Fecha	Descripción del cambio	Aprobación / Acto
1.0	18/11/2021	Emisión inicial de la política institucional de administración del riesgo. Incluye riesgos de gestión, corrupción y seguridad digital; adopta metodología DAFP (Guía v5.0), roles por líneas de defensa, periodicidades de reporte y lineamientos de comunicación.	Resolución No. 100 del 18/11/2021.
2.0	Marzo 2026	Ver anexo: Ajustes Política de Gestión de Riesgos DISTRISEGURIDAD	Por definir (Resolución/Acta No. ____ de ____/2026).

CONTENIDO

1. INTRODUCCIÓN

Distriseguridad, como establecimiento público descentralizado del Distrito de Cartagena de Indias, desarrolla su misión institucional mediante el apoyo logístico y tecnológico a la Alcaldía Distrital, a los organismos de seguridad y a la comunidad, orientado al mejoramiento de las condiciones de seguridad integral y convivencia en el territorio. En su direccionamiento institucional se reconoce, además, la importancia de la gestión de proyectos, la entrega oportuna de bienes y servicios, la administración de información y tecnología, el cumplimiento normativo y la atención a los grupos de valor.

En atención a su naturaleza misional, a su modelo de operación por procesos y a la responsabilidad institucional frente al adecuado uso de los recursos públicos, Distriseguridad adopta la presente Política de Gestión Integral del Riesgo como un instrumento rector para orientar la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos que puedan afectar el cumplimiento de sus objetivos, la continuidad de su gestión, la integridad institucional, la seguridad de la información, la confianza de la ciudadanía y la generación de valor público. Esta orientación responde al enfoque de la nueva guía del DAFP, que amplía la mirada desde la simple administración del riesgo hacia una gestión integral articulada con la planeación, el control interno y el desempeño institucional.

La presente política se formula en armonía con el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno – MECI, el esquema de líneas de defensa y los lineamientos establecidos por el Departamento Administrativo de la Función Pública para la gestión integral del riesgo en las entidades públicas. Así mismo, se alinea con el direccionamiento estratégico del Distrito de Cartagena y con el Plan de Desarrollo Cartagena Ciudad de Derechos, especialmente en su línea estratégica de Seguridad Humana, en la medida en que la misión de Distriseguridad aporta al fortalecimiento de capacidades tecnológicas, operativas e institucionales orientadas a la protección de la ciudadanía y al mejoramiento de las condiciones de seguridad y convivencia.

Esta política sustituye el enfoque adoptado en la política institucional vigente de 2021, que fue formulada con base en la guía versión 5 de 2020 y centrada principalmente en riesgos de gestión, corrupción y seguridad digital. La actualización busca simplificar el documento, eliminar repeticiones, separar los lineamientos estratégicos de los desarrollos metodológicos y adecuarlo a las nuevas exigencias sobre riesgos de gestión, riesgos fiscales, riesgos de seguridad de la información e integridad pública.

2. OBJETIVO

Establecer los lineamientos institucionales para la gestión integral del riesgo en Distriseguridad, con el fin de disminuir la vulnerabilidad frente a situaciones internas o externas que puedan interferir en el cumplimiento de su misión, objetivos estratégicos, procesos, planes, programas y proyectos, así como afectar la adecuada administración de los recursos públicos, la seguridad de la información, la integridad institucional y la confianza de la ciudadanía.

De manera específica, esta política busca orientar la gestión del riesgo en todos los niveles de la entidad, promover una cultura preventiva y de autocontrol, fortalecer la toma de decisiones basada en riesgos y contribuir al logro de los resultados institucionales, en concordancia con la Guía 2025 del DAFP.

3. ALCANCE

La presente política es de obligatorio cumplimiento para todos los procesos de Distriseguridad y aplica a los servidores públicos, contratistas, supervisores, directivos y demás colaboradores que intervengan en la planeación, ejecución, seguimiento, evaluación o apoyo de la gestión institucional.

Su alcance comprende los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad, así como los planes, programas, proyectos, actividades, recursos, activos de información, actuaciones administrativas y operaciones asociadas al cumplimiento de su misión. Igualmente, incluye los riesgos derivados de relaciones con terceros, operadores, contratistas, convenios, alianzas, apoyos tecnológicos y demás esquemas de articulación institucional que puedan generar impactos sobre la gestión de Distriseguridad.

La política abarca la gestión de riesgos de acuerdo con la naturaleza y necesidades de la entidad, incluyendo, entre otros, los riesgos de gestión, los riesgos fiscales, los riesgos de seguridad de la información, los riesgos asociados a la integridad pública y aquellos otros que, por la misión institucional y el entorno de operación de Distriseguridad, deban ser identificados y tratados de manera preventiva e integral.

4. ALINEACIÓN ESTRATÉGICA

La gestión integral del riesgo en Distriseguridad se fundamenta en un marco de referencia que integra la cultura, capacidades y prácticas institucionales con el direccionamiento estratégico, el ciclo de gestión presupuestal y el desempeño institucional. Su propósito fundamental es la creación y preservación de valor público, asegurando que la toma de decisiones en todos los niveles esté basada en la valoración objetiva de la incertidumbre.

La gestión integral del riesgo en Distriseguridad se enmarca en su naturaleza como establecimiento público descentralizado del Distrito de Cartagena, cuya finalidad es obtener, administrar, aplicar y controlar recursos de manera racional y transparente para apoyar logística y tecnológicamente a la Alcaldía Distrital, a los organismos de seguridad y a la comunidad, mediante proyectos y programas que contribuyan al mejoramiento de las condiciones de seguridad integral y convivencia.

En ese contexto, la política se articula con la plataforma estratégica institucional, con el modelo de operación por procesos y con los objetivos institucionales relacionados con la formulación y seguimiento de proyectos, la adquisición y supervisión de bienes y servicios, la administración de tecnología e información, la gestión financiera, la atención de peticiones y el cumplimiento normativo. La gestión del riesgo, por tanto, no constituye un ejercicio aislado, sino una herramienta transversal para proteger el cumplimiento de dichos objetivos y fortalecer el desempeño institucional.

De igual manera, esta política se alinea con el Plan de Desarrollo Cartagena Ciudad de Derechos 2024-2027, particularmente con la línea estratégica de *Seguridad Humana*, en la medida en que Distriseguridad contribuye al cumplimiento de dicha apuesta distrital mediante la formulación, gestión, adquisición, implementación, seguimiento y sostenibilidad de bienes, servicios, proyectos y soluciones tecnológicas orientadas al fortalecimiento de la seguridad y la convivencia en el territorio. Lo anterior comprende, entre otros, el apoyo a capacidades institucionales y operativas para el monitoreo, vigilancia, control, articulación con organismos de seguridad, gestión de información para la toma de decisiones y demás instrumentos tecnológicos que respaldan la acción

distrital en materia de prevención, respuesta y fortalecimiento de la seguridad ciudadana.

En consecuencia, la gestión integral del riesgo debe proteger no solo el cumplimiento de los objetivos internos de la entidad, sino también la efectiva entrega de los productos institucionales con los que Distriseguridad aporta a la ejecución de la línea estratégica de Seguridad Humana y a la generación de valor público para la ciudad.

5. CONTEXTO INTERNO Y EXTERNO

5.1. Contexto interno

Distriseguridad es un establecimiento público descentralizado del Distrito de Cartagena cuya misión es obtener, aplicar y controlar recursos de manera racional y transparente para apoyar logística y tecnológicamente a la Alcaldía Distrital, a los organismos de seguridad y a la comunidad, mediante proyectos y programas que contribuyan al mejoramiento de las condiciones de seguridad integral y convivencia. Su marco interno también evidencia objetivos estratégicos asociados a la formulación y seguimiento de proyectos, la adquisición, entrega y supervisión de bienes y servicios, la gestión de información, tecnología y comunicaciones, el manejo financiero, la atención de PQRS y el cumplimiento normativo.

La entidad opera bajo un modelo de operación por procesos conformado por doce procesos: uno estratégico, tres misionales, siete de apoyo y uno de evaluación. Entre ellos se destacan, por su incidencia en la exposición al riesgo, Gestión de Proyectos, Gestión Contractual, Entrega y Supervisión, Gestión TIC, Gestión Financiera, Atención al Ciudadano, Gestión Documental, Talento Humano y Control, Seguimiento y Evaluación. Esta estructura confirma que la gestión del riesgo debe incorporarse de forma transversal y no limitarse a un ejercicio documental de planeación.

Desde el punto de vista interno, Distriseguridad presenta una alta dependencia de capacidades tecnológicas y de coordinación interinstitucional. La naturaleza de su

misión implica administrar proyectos, bienes, servicios, infraestructura tecnológica, flujos de información y relaciones contractuales que soportan la seguridad ciudadana y la respuesta institucional. En la práctica reciente, esto se refleja en la operación o fortalecimiento de capacidades como CCTV, integración de cámaras, herramientas de monitoreo, drones, Titan, línea 123, Cívik y dotaciones tecnológicas para organismos de seguridad.

También existe una exposición interna relevante asociada a la gestión contractual y de supervisión, dado que buena parte del cumplimiento misional depende de adquisiciones, mantenimiento, operación de soluciones tecnológicas, soporte técnico, prestación de servicios y articulación con terceros. A ello se suman riesgos propios de la gestión pública: cumplimiento normativo, integridad, conservación documental, calidad de la información, continuidad operativa, suficiencia del talento humano y apropiación institucional de metodologías. Los documentos internos ya muestran que la entidad había reconocido riesgos por proceso y la necesidad de fortalecer cultura de riesgo, seguimiento y apropiación de herramientas institucionales.

Bajo este panorama, el contexto interno de Distriseguridad puede resumirse en cuatro rasgos estructurales:

- Primero: una misionalidad intensiva en tecnología;
- Segundo: una operación dependiente de proyectos, contratos y supervisión;
- Tercero: una necesidad permanente de articulación con actores externos;
- Cuarto: una exigencia alta en control, trazabilidad, integridad y disponibilidad de información. Estos factores hacen que la gestión integral del riesgo deba ser más robusta en riesgos operativos, fiscales, de seguridad de la información, de integridad pública y de continuidad institucional.

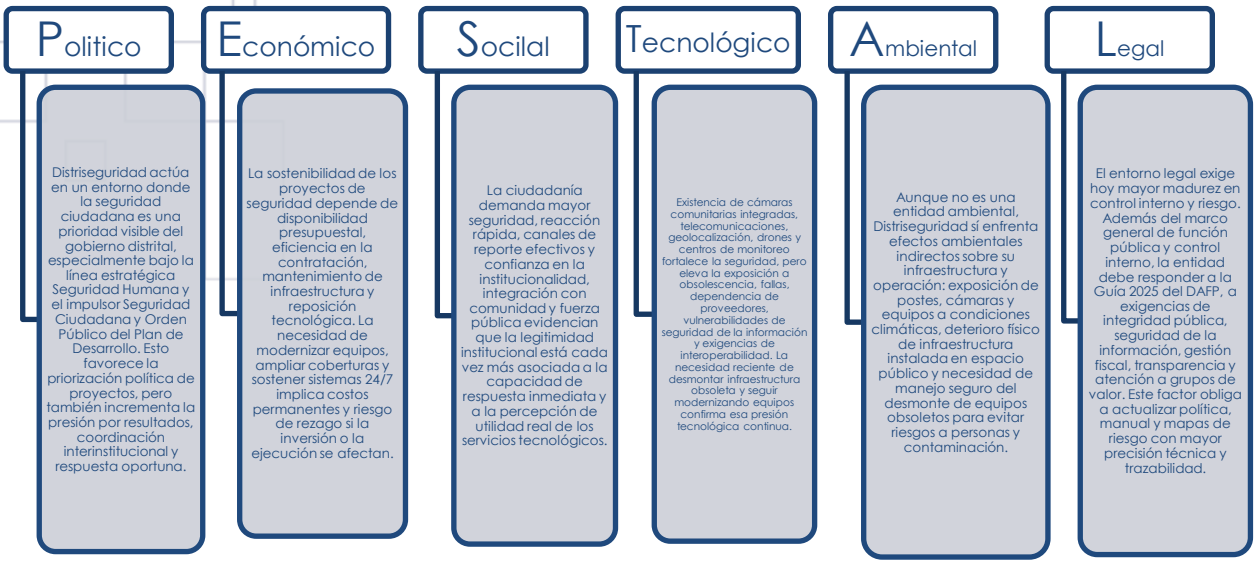
5.2. Contexto externo

El contexto externo de Distriseguridad está determinado por su inserción en el ecosistema de seguridad, convivencia, tecnología pública y gestión territorial del Distrito de Cartagena. La entidad no actúa de manera aislada: su operación se relaciona con la Alcaldía Mayor, la Secretaría del Interior y Convivencia, la Policía Metropolitana, organismos de socorro, entes de control, contratistas, ciudadanía, sector privado y comunidades que participan directa o indirectamente en esquemas de vigilancia, reporte, prevención y respuesta.

En el plano estratégico, el principal marco externo es el Plan de Desarrollo Cartagena, Ciudad de Derechos 2024–2027, cuya línea Seguridad Humana busca proteger la vida frente a distintos factores de riesgo y se desarrolla, entre otros, mediante el impulsor Seguridad Ciudadana y Orden Público. El seguimiento distrital más reciente reporta que este componente ha mostrado un desempeño alto, aunque todavía con desafíos de sostenibilidad y articulación, lo que implica presión positiva sobre las entidades que contribuyen a su ejecución, entre ellas Distriseguridad.

Además, el entorno externo está fuertemente marcado por la aceleración tecnológica y por mayores expectativas de respuesta en tiempo real. La operación pública reciente

en Cartagena evidencia una orientación hacia seguridad apoyada en tecnología, integración de cámaras públicas y comunitarias, geolocalización, canales digitales de reporte y monitoreo 24/7. Ese mismo avance genera beneficios, pero también incrementa la exposición a riesgos de disponibilidad, ciberseguridad, mantenimiento, interoperabilidad, protección de datos, dependencia tecnológica y reputación institucional cuando los sistemas no responden adecuadamente.



6. GLOSARIO

Para efectos de esta política, se adoptan las siguientes definiciones (las cuales se complementan con las definiciones de la Guía DAFP vigente y marcos ISO aplicables):

Término	Definición
Riesgo	Efecto que se causa sobre los objetivos institucionales debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
Gestión del riesgo	Proceso efectuado por la Alta Dirección y por todo el personal para proporcionar un

	aseguramiento razonable con respecto al logro de los objetivos institucionales.
Riesgo de gestión	Posibilidad de que suceda un evento que tenga un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
Riesgo de seguridad de la información	Posibilidad de que una amenaza concreta explote una vulnerabilidad y cause una pérdida o daño en un activo de información. Suele considerarse como combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).
Riesgo de seguridad digital	Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar intereses nacionales. Incluye aspectos del ambiente físico, digital y las personas.
Riesgos para la integridad pública	Riesgos que pueden afectar la transparencia, ética pública y confianza ciudadana (por ejemplo: soborno, fraude, conflicto de intereses, corrupción), y que se gestionan de forma articulada con el PTEP/SIGRIP, cuando aplique.
Activo	Elemento que utiliza la organización para funcionar (aplicaciones, servicios web, redes, hardware, información física o digital, recurso humano, entre otros) y que debe protegerse según su criticidad.
Causa	Factores internos o externos que, solos o en combinación, pueden producir la materialización de un riesgo.
Causa inmediata	Circunstancias bajo las cuales se presenta el riesgo, pero que no constituyen la causa principal.
Causa raíz	Causa principal o básica: razones por las cuales se puede presentar el riesgo. Es base para definir controles.
Factores de riesgo	Fuentes generadoras de riesgos (por ejemplo: personas, procesos, tecnología, infraestructura, factores externos).

Consecuencia	Efectos o situaciones resultantes de la materialización del riesgo que impactan el proceso, la entidad y sus grupos de valor.
Probabilidad	Posibilidad de ocurrencia del riesgo. Puede medirse con criterios de frecuencia o factibilidad.
Impacto	Consecuencias que puede ocasionar a la organización la materialización del riesgo.
Nivel de riesgo	Valor determinado al combinar probabilidad e impacto (por ejemplo: Probabilidad x Impacto, o matriz de calor).
Riesgo inherente	Riesgo al que se enfrenta la entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
Riesgo residual	Nivel de riesgo que permanece luego de aplicar medidas de tratamiento y controles.
Mapa de riesgos	Documento o registro que consolida la información resultante de la gestión del riesgo (riesgos, causas, controles, responsables, niveles y tratamientos).
Control	Medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones). Puede ser preventivo, detectivo o correctivo; manual o automático.
Amenaza	Causa potencial de un incidente no deseado que puede ocasionar daño a un sistema o a una organización.
Vulnerabilidad	Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
Confidencialidad	Propiedad de la información que la hace no disponible o no divulgada a individuos, entidades o procesos no autorizados.
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Tolerancia al riesgo	Niveles aceptables de desviación relativa a la consecución de objetivos. Para riesgos asociados a actos de corrupción/violaciones graves de integridad pública, la tolerancia es inaceptable.

Apetito del riesgo	Magnitud y tipo de riesgo que la organización está dispuesta a buscar o retener.
Capacidad de riesgo	Máximo nivel de riesgo que la entidad puede soportar; a partir del cual la Alta Dirección considera que no sería posible el logro de objetivos.
KPI - Indicador clave de riesgo	Métrica basada en datos históricos por periodos de tiempo, cuyo comportamiento puede indicar mayor o menor exposición. No implica materialización del riesgo, pero sugiere desviaciones que deben investigarse.
KPI - Indicador clave de desempeño	Métrica que mide resultados o cumplimiento de objetivos. Se articula con KPI para monitorear desempeño y riesgo.

6.1. Abreviaturas

Abreviaturas utilizadas en el documento:

- CICCI: Comité Institucional de Coordinación de Control Interno
- CIGD: Comité Institucional de Gestión y Desempeño
- DAFP: Departamento Administrativo de la Función Pública
- MECI: Modelo Estándar de Control Interno
- MIPG: Modelo Integrado de Planeación y Gestión
- SIG: Sistema Integrado de Gestión
- MSPI: Modelo de Seguridad y Privacidad de la Información (Gobierno Digital - MinTIC)
- TIC: Tecnologías de la Información y las Comunicaciones
- PTEP: Programa de Transparencia y Ética Pública
- SIGRIP: Sistema de Gestión de Riesgos para la Integridad Pública
- SLA: Acuerdo de niveles de servicio (Service Level Agreement)

7. MARCO NORMATIVO

La presente política se formula considerando, entre otros, los siguientes referentes. La lista es orientadora y no limita la aplicación de otra norma o lineamiento aplicable.

Principales referentes normativos y técnicos (orientador):

Norma / Referente	Aplicación en la política
Ley 1474 de 2011	Normas orientadas a fortalecer mecanismos de prevención, investigación y sanción de actos de corrupción; incluye lineamientos para planes/estrategias anticorrupción.
Ley 1712 de 2014	Ley de transparencia y acceso a la información pública, relevante para publicación de información y gestión de información clasificada o reservada.
Ley 2195 de 2022	Medidas de transparencia, prevención y lucha contra la corrupción (marco para integridad pública).
Decreto 1083 de 2015	Decreto Único Reglamentario del Sector Función Pública; compila normas relacionadas con función pública y gestión institucional.
Decreto 124 de 2016	Lineamientos para la estrategia de lucha contra la corrupción y atención al ciudadano (antecedente).
Decreto 1499 de 2017	Modifica el Decreto 1083 de 2015 y adopta el Modelo Integrado de Planeación y Gestión (MIPG) v2.
Decreto 1122 de 2024	Reglamenta Programas de Transparencia y Ética Pública (PTEP) e integra el Anexo Técnico asociado al enfoque programático; incorpora el SIGRIP como referente.
Guía DAFP para la gestión integral del riesgo en entidades públicas (v7 - 2025)	Marco metodológico para gestión integral del riesgo, incluyendo riesgo fiscal, seguridad de la información e integridad pública (SIGRIP).
Guía DAFP para administración del riesgo y diseño de controles (v5 - 2020)	Antecedente metodológico adoptado en la versión 1.0; se mantiene como referencia histórica y de transición cuando aplique.

ISO 9001:2015 (Cap. 6.1)	Lineamientos para identificar, controlar y evaluar riesgos y oportunidades para mejora continua.

8. ROLES Y RESPONSABILIDADES

8.1. Esquema de Líneas de Aseguramiento

Distriseguridad adopta el Esquema de Líneas de Aseguramiento como marco para asignación de responsabilidades en la gestión del riesgo y el control.

A continuación, se describen responsabilidades mínimas por línea (la entidad podrá ampliar según su reglamento interno):

Línea	Responsables	Responsabilidades en la gestión del riesgo
Línea Estratégica	Corresponde a la Dirección General y a las instancias directivas y comités institucionales competentes, en especial el Comité Institucional de Coordinación de Control Interno, en cuanto les corresponda.	• Aprobar la Política de Gestión Integral del Riesgo y sus actualizaciones. • Definir y revisar el apetito, la tolerancia y los criterios generales de aceptación del riesgo. • Analizar los cambios del contexto interno y externo que puedan afectar la operación institucional y la estructura de riesgos. • Hacer seguimiento periódico al estado de los riesgos institucionales y a las acciones definidas para su tratamiento. • Impulsar una cultura institucional orientada a la prevención, la integridad, el autocontrol y la mejora continua.

		Estas funciones guardan relación con los roles que ya tenía definida la entidad para la línea estratégica.
Primera línea	Está conformada por los líderes de proceso, responsables de planes, programas y proyectos, supervisores y equipos de trabajo que ejecutan la operación institucional.	• Identificar, analizar, valorar y actualizar los riesgos en el ámbito de su gestión. • Diseñar, aplicar y hacer seguimiento a los controles y acciones de tratamiento. • Reportar oportunamente riesgos materializados, cambios relevantes y necesidades de ajuste. • Generar y conservar evidencias del seguimiento a los riesgos y controles. • Incorporar la gestión del riesgo en la planeación y ejecución de las actividades
Segunda línea	Le Corresponde principalmente a la dependencia responsable de Planeación, como instancia articuladora y orientadora de la gestión integral del riesgo en Distriseguridad. En desarrollo de este rol, le corresponde liderar metodológicamente la implementación de la política, promover su articulación con la planeación institucional, coordinar la consolidación del mapa institucional de riesgos y realizar monitoreo sobre la gestión adelantada por la primera línea de defensa.	• Liderar técnicamente la implementación de la Política de Gestión Integral del Riesgo en la entidad. • Definir, actualizar y socializar lineamientos, herramientas e instrumentos metodológicos para la gestión integral del riesgo. • Asesorar y acompañar a los líderes de proceso en la identificación, análisis, valoración, tratamiento, monitoreo y actualización de los riesgos. • Coordinar la consolidación, revisión y actualización del mapa institucional de riesgos. • Realizar monitoreo a la gestión adelantada por la primera línea de defensa y generar alertas o

		recomendaciones cuando corresponda. • Presentar reportes e informes a la alta dirección y a las instancias institucionales competentes sobre el estado de la gestión del riesgo. • Promover la articulación entre los riesgos de gestión, fiscales, de seguridad de la información, de integridad pública y demás tipologías aplicables. • Impulsar acciones de fortalecimiento de capacidades, apropiación metodológica y cultura institucional en materia de gestión integral del riesgo.
Tercera línea	Corresponde a la Oficina de Control Interno o quien haga sus veces. Son responsabilidades de la tercera línea	• Proporcionar aseguramiento independiente y objetivo sobre la efectividad de la gestión del riesgo y de los controles. • Evaluar la idoneidad del diseño y funcionamiento de los controles. • Realizar seguimiento en el marco del plan anual de auditoría. • Formular recomendaciones de mejora a la política, al manual metodológico y a la gestión institucional del riesgo.

La gestión integral del riesgo es una responsabilidad de todos los niveles de la organización y no se limita a las oficinas de planeación o control interno. Cada servidor y colaborador de Distriseguridad asume el compromiso de actuar bajo una cultura de autocontrol, reportando proactivamente señales de alerta y riesgos materializados para fortalecer el ambiente de integridad institucional.

9. LINEAMIENTOS GENERALES PARA LA GESTIÓN INTEGRAL DEL RIESGO

Distriseguridad desarrollará la gestión integral del riesgo como un proceso continuo, sistemático y articulado con la planeación institucional, el modelo de operación por procesos y el sistema de control interno. Para ello se adoptan los siguientes lineamientos generales:

9.1. Identificación del riesgo.

Cada proceso, plan, programa o proyecto deberá identificar los eventos potenciales que puedan afectar el cumplimiento de sus objetivos, considerando causas, consecuencias, contexto interno y externo, actores relacionados, activos involucrados y posibles impactos sobre la entidad, la ciudadanía y el patrimonio público.

9.2. Análisis y valoración.

Los riesgos identificados deberán ser analizados y valorados con base en criterios metodológicos institucionales, atendiendo su probabilidad, impacto, controles existentes y nivel residual, conforme a la tipología de riesgo aplicable.

La gestión preventiva de riesgos fiscales en la entidad tiene como fin primordial evitar el daño patrimonial, entendido como el menoscabo, perjuicio, detrimento o pérdida de los bienes y recursos públicos administrados por Distriseguridad. La identificación de estos riesgos se basará en el análisis de puntos críticos de la gestión fiscal y precedentes de fallos de responsabilidad fiscal.

9.3. Tratamiento del riesgo.

La entidad definirá acciones de tratamiento orientadas a evitar, reducir, compartir, asumir controladamente o gestionar de manera diferenciada los riesgos, priorizando aquellos que tengan mayor criticidad o que puedan comprometer el logro de los objetivos institucionales, la integridad pública, la información o los recursos públicos.

9.4. Monitoreo y seguimiento.

Los riesgos y controles deberán ser objeto de monitoreo periódico por parte de la primera y segunda línea de defensa, y de evaluación independiente por parte de la tercera línea. El seguimiento deberá considerar cambios del entorno, materialización de riesgos, efectividad de controles y necesidad de ajustes.

9.5. Reporte y escalamiento.

Los riesgos críticos, materializados o que superen los niveles definidos por la entidad deberán ser reportados oportunamente a las instancias correspondientes, con el fin de adoptar decisiones, activar acciones de mejora y revisar el mapa de riesgos cuando sea necesario.

9.6. Articulación metodológica.

La política fija lineamientos generales; la metodología específica, escalas, herramientas, formatos y criterios diferenciales por tipología de riesgo se desarrollarán en el anexo metodológico institucional.

9.7. Actualización permanente.

La gestión del riesgo deberá actualizarse cuando existan cambios relevantes en la estructura institucional, la planeación estratégica, la normatividad aplicable, el entorno tecnológico, los procesos, los responsables, los controles o las condiciones del entorno externo.

9.8 Identificación de Riesgos Emergentes:

La entidad, dada su naturaleza intensiva en tecnología, implementará mecanismos para la detección temprana de riesgos emergentes asociados a cambios tecnológicos disruptivos, nuevas ciber amenazas, variaciones normativas y transformaciones del entorno que puedan afectar la continuidad del servicio o la seguridad de la entidad.

10. APETITO, TOLERANCIA Y ACEPTACIÓN DEL RIESGO

Distriseguridad reconoce que la gestión integral del riesgo requiere definir criterios institucionales claros sobre el nivel de riesgo que está dispuesta a asumir en el desarrollo de su misión, dentro del marco legal aplicable y bajo las orientaciones de la alta dirección.

Para efectos de esta política, se adoptan las siguientes referencias conceptuales:

- **Apetito del riesgo:** nivel de riesgo que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección.
- **Tolerancia del riesgo:** máxima desviación admisible del nivel de riesgo respecto del apetito definido por la entidad.
- **Capacidad de riesgo:** máximo nivel de riesgo que la entidad puede soportar sin comprometer de manera grave su capacidad para cumplir sus objetivos.

Con base en ello, Distriseguridad adoptará los siguientes lineamientos:

10.1. Definición institucional.

La Alta Dirección establece que para Distriseguridad el apetito de riesgo es mínimo o cero en las tipologías de Integridad Pública (SIGRIP) y Riesgos Fiscales. Para los riesgos de gestión y seguridad de la información, se definirán umbrales de alerta a través de

Indicadores Clave de Riesgo (KRI), los cuales activarán acciones correctivas inmediatas cuando se supere la desviación admisible establecida en el anexo metodológico

10.2. Criterio general de aceptación.

La entidad podrá asumir riesgos residuales únicamente cuando estos se encuentren dentro de los niveles definidos como aceptables y no comprometan el cumplimiento misional, la legalidad, la integridad, la seguridad de la información, la confianza institucional ni la protección del patrimonio público.

10.3. Riesgos no aceptables.

Distriseguridad no aceptará riesgos que puedan derivar en:

- Afectación grave al patrimonio público.
- Vulneraciones significativas a la integridad pública.
- Incumplimiento normativo relevante.
- Afectación crítica a la confidencialidad, integridad o disponibilidad de la información.
- Interrupción grave de la operación misional.
- Daño reputacional severo por actuaciones contrarias al interés general.

10.4. Diferenciación por tipologías.

El apetito del riesgo podrá variar según la tipología de riesgo y según el proceso o actividad.

10.5. Desarrollo metodológico.

Los criterios, umbrales, escalas y mecanismos de evaluación del apetito, tolerancia y capacidad del riesgo serán desarrollados en el anexo metodológico institucional.

11. SEGUIMIENTO, MONITOREO Y MEJORA

La gestión integral del riesgo en Distriseguridad será objeto de seguimiento, monitoreo y revisión permanente, con el propósito de verificar la efectividad de los controles, la pertinencia de las acciones de tratamiento, la actualización del mapa de riesgos y la capacidad institucional para anticipar y responder a eventos que puedan afectar el cumplimiento de su misión, objetivos y compromisos institucionales.

El seguimiento al riesgo deberá desarrollarse de manera articulada entre las líneas de defensa, de acuerdo con sus responsabilidades, y considerar como mínimo: la evolución del riesgo inherente y residual, la efectividad de los controles, el cumplimiento de las acciones de tratamiento, la materialización de eventos, la identificación de riesgos emergentes, los cambios del contexto interno y externo y la necesidad de ajustar las valoraciones o medidas adoptadas.

- La primera línea de defensa realizará seguimiento periódico a los riesgos bajo su responsabilidad y dejará evidencia de la ejecución de controles, del avance de las acciones de tratamiento y de las situaciones que requieran ajuste o escalamiento.

- La segunda línea de defensa consolidará, acompañará y monitoreará la información reportada por los procesos, generará alertas cuando corresponda y presentará reportes a la alta dirección y a las instancias institucionales competentes para apoyar la toma de decisiones.

- La tercera línea de defensa, en el marco de su rol de evaluación independiente, verificará la efectividad del sistema de control interno y de la gestión del riesgo,

formulará recomendaciones de mejora y realizará el seguimiento correspondiente conforme a su plan anual de auditoría.

Cuando se materialice un riesgo, se identifiquen debilidades significativas en los controles o se presenten cambios relevantes en el contexto institucional, normativo, tecnológico, contractual u operativo, los líderes de proceso y responsables correspondientes deberán analizar la situación, definir las acciones de respuesta y promover la actualización del mapa de riesgos y de los controles asociados.

La entidad promoverá la mejora continua de la gestión integral del riesgo mediante ejercicios de revisión periódica de la política, del anexo metodológico, de los mapas de riesgo y de los instrumentos de seguimiento, teniendo en cuenta los resultados del monitoreo, las recomendaciones de control interno, los cambios normativos y las lecciones aprendidas derivadas de la operación institucional.

12. DISPOSICIONES FINALES

La presente Política de Gestión Integral del Riesgo rige a partir de su aprobación por la instancia competente de Distriseguridad y deroga las disposiciones internas que le sean contrarias, en especial aquellas contenidas en la política institucional de administración del riesgo adoptada con anterioridad, en lo que resulte incompatible con el nuevo enfoque de gestión integral del riesgo.

La política deberá ser socializada e implementada en todos los procesos de la entidad y será de obligatorio cumplimiento para servidores públicos, contratistas, supervisores, directivos y demás colaboradores que intervengan en la gestión institucional.

Los aspectos metodológicos, criterios técnicos, escalas de valoración, formatos, matrices, herramientas y lineamientos específicos para la identificación, análisis, valoración, tratamiento y seguimiento de las distintas tipologías de riesgo serán desarrollados en el anexo metodológico de gestión integral del riesgo, el cual deberá mantenerse articulado con la presente política y con la Guía vigente del Departamento Administrativo de la Función Pública.

La política será revisada periódicamente y deberá actualizarse cuando se presenten modificaciones en el marco normativo, en los lineamientos nacionales aplicables, en la estructura institucional, en la plataforma estratégica, en el modelo de operación por procesos, en las condiciones del entorno o en cualquier otro aspecto que incida de manera relevante en la gestión del riesgo de Distriseguridad.

La dependencia encargada de liderar técnicamente la gestión integral del riesgo promoverá las acciones de articulación, acompañamiento y seguimiento requeridas

para asegurar la implementación efectiva de esta política y su incorporación en la gestión institucional.