Igualdad

POLITICA DE ADMINISTRACIÓN DE RIESGOS 05/06/2026

Versión No 2

Contenido

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

INTRODUCCIÓN

La gestión integral del riesgo constituye un componente estratégico para el fortalecimiento institucional, la generación de valor público y el cumplimiento de los objetivos misionales del Ministerio de Igualdad y Equidad. En este sentido, la presente Política de Gestión Integral de Riesgos establece los lineamientos para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales, la adecuada administración de los recursos públicos, la integridad pública, la seguridad de la información y la prestación de los servicios a la ciudadanía.

La política se fundamenta en los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo Estándar de Control Interno (MECI), la Guía para la Gestión Integral del Riesgo en Entidades Públicas versión 7 de 2025 emitida por el Departamento Administrativo de la Función Pública (DAFP) y las demás disposiciones aplicables en materia de integridad pública, transparencia, control interno, seguridad digital y lucha contra la corrupción. En concordancia con la Guía V7, el Ministerio adopta un enfoque integral, preventivo y basado en riesgos, articulado con el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), incorporando lineamientos para la gestión de riesgos de gestión, integridad pública, corrupción, fraude, soborno, conflictos de interés, riesgos fiscales, seguridad de la información y riesgos asociados al lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva (LA/FT/FP).

La gestión integral del riesgo se desarrollará bajo el esquema de líneas de defensa y será aplicable a todas las dependencias, procesos, planes, programas, proyectos, direcciones territoriales, personas servidoras públicas, contratistas y demás actores vinculados a la gestión institucional. Así mismo, promoverá el fortalecimiento de la cultura institucional orientada a la prevención, el autocontrol, la debida diligencia, la transparencia y la mejora continua, contribuyendo a la protección de los recursos públicos, la confianza ciudadana y el cumplimiento efectivo de la misión institucional.

1. OBJETIVO GENERAL

Implementar el Sistema Integrado de Gestión de Riesgos Institucionales mediante la adopción de lineamientos, metodologías, herramientas y controles establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas versión 7 de 2025, con el fin de fortalecer la administración efectiva de los riesgos de gestión, integridad pública, corrupción, fraude, soborno, conflictos de interés, lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva (LA/FT/FP), riesgos fiscales y riesgos de seguridad de la información, contribuyendo al cumplimiento de los objetivos estratégicos institucionales, la protección de los recursos públicos y la generación de valor público.

1.1. Objetivos Específico

- Comunicar a todos los niveles del Ministerio los lineamientos, metodologías y directrices para la gestión integral de riesgos, con el fin de fortalecer su apropiación y aplicación en los procesos institucionales.
- Fortalecer la cultura institucional de prevención y gestión del riesgo mediante estrategias de sensibilización, capacitación y acompañamiento técnico dirigidas a los servidores públicos, contratistas y demás partes interesadas.
- Definir las responsabilidades y líneas de actuación frente a la gestión integral de riesgos, conforme al modelo de líneas de defensa y a las competencias institucionales establecidas en el SIG-MIPG.
- Identificar, analizar y gestionar las amenazas y vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles y mecanismos de gestión de riesgos de seguridad de la información.

2. ALCANCE

La Política de Gestión Integral de Riesgos Institucionales aplica a todas las dependencias, procesos, planes, programas, proyectos, trámites, servicios y actividades

desarrolladas por el Ministerio de Igualdad y Equidad, incluidas las direcciones territoriales y los procesos estratégicos, misionales, de apoyo, evaluación y control. Así mismo, aplica a todos los servidores públicos, contratistas, terceros, operadores y demás actores que intervengan en la gestión institucional, independientemente de su modalidad de vinculación o ubicación territorial.

El alcance de la presente política comprende la gestión integral de riesgos de gestión, integridad pública, corrupción, fraude, soborno, conflictos de interés, lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva (LA/FT/FP), riesgos fiscales y riesgos de seguridad de la información, conforme a los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo Estándar de Control Interno (MECI), el Sistema Integrado de Gestión y el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, incorporando actividades de identificación, análisis, valoración, tratamiento, monitoreo, seguimiento y control de los riesgos institucionales.

3 DEFINICIONES Y SIGLAS

Para efectos de la presente Política de Gestión Integral de Riesgos Institucionales, se establecen las siguientes definiciones y siglas, con el propósito de unificar criterios conceptuales y facilitar la interpretación, aplicación, seguimiento y control de la presente política institucional:[1]

Activo de información: En relación con la seguridad de la información como los datos, los sistemas de información (software y hardware), se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas etc) que tenga valor para la organización.

Actividad de control: Son las acciones establecidas a través de políticas y

[1] Las definiciones y términos contenidos en el presente documento fueron adoptados y adaptados con fundamento en las guías y lineamientos emitidos por el Departamento Administrativo de la Función Pública (DAFP), el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), normas técnicas ISO aplicables y demás referentes técnicos y normativos relacionados con la gestión integral de riesgos, seguridad de la información e integridad pública.

procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.
Amenazas: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Amenaza informática: Situación potencial o actual que tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Análisis de Riesgo: Determinar el impacto y la probabilidad del riesgo, dependiendo de la información disponible pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.

Apetito al riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales.
Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques.

Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

COLCERT/CSIRT: Es un equipo especializado en la respuesta a incidentes de seguridad informática que coordina la ciberseguridad nacional pública y privada. Su alcance es la responsabilidad sobre la seguridad digital de la nación y quienes coordinan las respuestas de los incidentes que podrían afectar la infraestructura tecnológica nacional.

Confidencialidad: Propiedad que garantiza que la información sea accesible únicamente a personas, entidades o procesos no autorizados, protegiéndola contra divulgación o acceso no autorizado.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Fraude: Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Gestión del riesgo: Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto

al logro de los objetivos.

ICC: Es la denominación de lo que el CCOCI ha definido como Infraestructuras Críticas Cibernéticas en el ámbito colombiano.

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Información: Es un activo de valor o conjunto de datos procesados y organizados que hace parte del Ministerio, por la cual asume funciones como responsable o encargada de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato de la entidad (tecnológico, administrativo, financiero, contable, entre otros), propio o de Terceros con las cuales dispone de un acuerdo o convenio; y datos personales de las cuales asume un rol como responsable o encargado

Integridad: Propiedad de la información de ser exacta y completa.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas, entre otras.

Indicadores Clave de Riesgo (KRI): son métricas utilizadas por la Entidad para proporcionar una señal temprana de exposiciones al riesgo, cada vez mayores en diversas áreas, proporcionan información oportuna sobre riesgos emergentes y potenciales que pueden tener impacto sobre el logro de los objetivos de la organización,

así como las medidas en las cuales diferentes eventos o puntos desencadenantes, pueden ofrecer información valiosa a la alta dirección de la entidad para tomar las medidas correctivas y preventivas para mitigar los riesgos y velar por el cumplimiento de los objetivos establecidos[2].

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.

Líder o responsable del proceso: Persona con la responsabilidad y autoridad para gestionar un riesgo.

Mapa de Riesgos: Documento con la información resultante de la gestión del riesgo.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Plan de contingencia: Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.

Plan de manejo del riesgo: Plan de acción propuesto por el grupo de trabajo interno, cuya evaluación de beneficio costo resulta positiva y es aprobado por la Alta Dirección.

Política de Administración de Riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4 / ISO 27001). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

[2] Adaptado de DAFP Guía para la Gestión Integral del Riesgo en Entidades Públicas 2025 V.7

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Seguridad de la información: Conjunto de medidas que buscan la protección de la información física, electrónica, digital del acceso, uso, divulgación o destrucción no autorizada que permite cumplir leyes y regulaciones (como la ISO 27001), la seguridad de la información cuenta con tres pilares fundamentales que son: confidencialidad, integridad y disponibilidad de la información.

Recurso Público: entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por eficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la Infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Fraude: Efecto que se causa sobre los objetivos de las entidades debido a una acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Riesgo de Gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de Seguridad Digital: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001).

Riesgos Emergentes: Son aquellos riesgos nuevos, cambiantes o en evolución, de difícil anticipación, que surgen por transformaciones tecnológicas, sociales, ambientales, económicas, normativas o políticas, y que tienen el potencial de afectar a mediano o largo plazo el cumplimiento de los objetivos estratégicos y la generación de valor público de la Entidad.

Riesgo Fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Tolerancia al riesgo (niveles de aceptación): Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes, que específicamente para el riesgo de corrupción la tolerancia es ***inaceptable.***

Valorar el riesgo: Permite establecer la probabilidad de ocurrencia del riesgo y el nivel

de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial. (Riesgo Inherente).

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

Lavado de Activos (LA): catalogado como delito, es aquella acción mediante la cual personas u organizaciones intentan dar apariencia de legalidad a recursos provenientes de actividades ilícitas, como el narcotráfico o la corrupción.

Financiación del Terrorismo (FT): Es el acto de proporcionar dinero, recursos servicios destinados total o parcialmente a financiar actividades terroristas.
Financiación de la Proliferación de Armas de Destrucción Masiva (FPADM) Actos que facilitan la obtención de recursos, materiales o tecnología para apoyar programas de proliferación o actores sancionados internacionalmente.

Operación Sospechosa (OS): Actividad, transacción, conducta o comportamiento inusual, inconsistente o sin justificación económica, jurídica o técnica aparente, que podría estar vinculada a LA/FT/FPADM.

Soborno: es una conducta en la que se entregue o prometa dinero u otra utilidad a un testigo para que falte a la verdad o la calle total o parcialmente en su testimonio (Estatuto Anticorrupción, 2011).

Persona políticamente expuesta (PEP): Es un individuo que ocupa o ha ocupado un cargo público importante, así como sus familiares y asociados cercanos. Las PEP son consideradas de mayor riesgo en el ámbito del lavado de activos y la financiación del terrorismo debido a su posición de influencia y al acceso a recursos públicos.

4. MARCO NORMATIVO

La gestión de riesgos en el sector público en Colombia se enmarca en un conjunto de legislaciones y normativas que regulan y guían las prácticas de gestión de riesgos. A continuación, se detallan las principales normativas aplicables:

Ley 87 de 1993 en el Artículo 2º, literal a. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
Ley 1474 de 2011. Estatuto Anticorrupción.
Ley 1712 de 2014. Ley de transparencia y acceso a la información pública.
Decreto 1081 de 2015. Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.
Decreto 1083 de 2015, artículo 2.2.21.5.4 Administración de riesgos**.**
Decreto 1499 de 2017. Actualiza el Modelo Estándar de Control Interno (MECI).
Decreto 1122 de 2024. Programas de Transparencia y Ética Pública (PTEP).
CONPES 3854 de 2026. Política Nacional de Seguridad Digital Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. Esta ley resalta la importancia de la gestión de riesgos como parte integral del control interno.
CONPES 4042 de 2021. Política Nacional Antilavado de Activos y Contra la Financiación del Terrorismo.

DOCUMENTOS TÉCNICOS

- Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 de 2025, emitida por el Departamento Administrativo de la Función Pública – DAFP.
- Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG.
- Lineamientos del Modelo Nacional de Gestión del Riesgo de Seguridad de la Información – MSPI versión 5.0 de 2025, emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Directiva Presidencial 003 de 2021, relacionada con servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Guías y lineamientos emitidos por la Secretaría de Transparencia de la Presidencia de la República en materia de integridad pública y SIGRIP.
- Protocolo para la Identificación de Riesgos de Corrupción Asociados a Trámites y Servicios – DAFP.
- NTC-ISO 31000:2018 – Gestión del Riesgo. Principios y directrices.

- NTC-ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información.
- ISO 37001 – Sistemas de Gestión Antisoborno.
- COSO ERM 2017 – Enterprise Risk Management Framework.

5. POLÍTICA PARA LA ADMINISTRACIÓN DE RIESGOS

5.1 Política general

El Ministerio de la Igualdad y Equidad está comprometido con llevar a cabo una gestión integral de riesgos que facilite el cumplimiento de la misión, los objetivos estratégicos, objetivos de los procesos y la satisfacción de los grupos de interés, llevando a cabo la identificación de riesgos de gestión por proceso, los riesgos de integridad, riesgos de seguridad de la información, riesgos fiscales, análisis, valoración y formulación de los planes de tratamiento de riesgos o acciones para prevenir su ocurrencia o mitigar el impacto. Las políticas de manejo de riesgo aplican a todos los procesos de la entidad incluidas las direcciones territoriales, se establecen las opciones para el tratamiento de los riesgos. Los riesgos de integridad (corrupción) son inaceptables y en consecuencia no se pueden asumir. El tratamiento general para los riesgos corresponde a la implementación de acciones que conlleven a reducir, evitar, compartir, aceptar o transferir y serán individuales para cada uno de los riesgos identificados. Las acciones o controles se formularán considerando su viabilidad técnica, económica y legal.
Política del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP).

5.1.1 Política del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP)

El Ministerio de Igualdad y Equidad adopta el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), como instrumento institucional orientado a prevenir, identificar, analizar, controlar, monitorear y tratar los riesgos que puedan afectar la integridad pública, la transparencia, la ética institucional, la adecuada administración de los recursos públicos y el cumplimiento de los objetivos estratégicos y misionales de la Entidad.

En desarrollo de esta política, el Ministerio promoverá una cultura institucional basada en los mandatos rectores de legalidad, transparencia, responsabilidad, moralidad

administrativa, debida diligencia, prevención del daño antijurídico y prevalencia del interés general. Asimismo, se fortalecerán los mecanismos para la gestión de riesgos asociados a corrupción, soborno, fraude, conflictos de interés, lavado de activos, financiación del terrorismo, financiación de la proliferación de armas de destrucción masiva (LA/FT/FP) y demás factores que puedan comprometer la confianza pública o la integridad institucional.

El SIGRIP se articulará con el Modelo Integrado de Planeación y Gestión (MIPG), el Programa de Transparencia y Ética Pública (PTEP), el Sistema de Control Interno, el Sistema Integrado de Gestión, la Política de Integridad Institucional y el modelo de líneas de defensa, incorporando mecanismos de debida diligencia, gestión de contrapartes, canales de denuncia, monitoreo de riesgos, seguimiento a controles, función de cumplimiento y acciones de mejora continua.

Todas, todos y todes las, los y les servidores públicos, contratistas, directivos, terceros y demás personas vinculadas a la gestión institucional deberán actuar conforme a los criterios y lineamientos establecidos en la presente política, reportando oportunamente cualquier situación irregular, señal de alerta o conducta contraria a la integridad pública. El incumplimiento de estos lineamientos dará lugar a las acciones administrativas, disciplinarias, fiscales, contractuales y penales a que haya lugar, conforme a la normatividad vigente.

5.1.2 Política ALA/CFT/CFP

El Ministerio de Igualdad y Equidad manifiesta su compromiso institucional con la prevención del lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva (LA/FT/FP), rechazando cualquier práctica, operación o conducta que pueda facilitar el uso indebido de recursos públicos, afectar la integridad institucional o comprometer el cumplimiento de la normatividad vigente.

En desarrollo de esta política, el Ministerio implementará mecanismos de debida diligencia para el conocimiento y análisis de las contrapartes, personas beneficiarias, firmas proveedoras, el equipo contratista, las y los operadores y las, los y les demás

terceros vinculados a la gestión institucional. Asimismo, se incorporarán medidas orientadas a la identificación de señales de alerta, monitoreo de operaciones inusuales, reporte oportuno de situaciones sospechosas y fortalecimiento de controles preventivos y detectivos asociados a riesgos LA/FT/FP.

De igual manera, la Entidad garantizará canales de denuncia y reporte confidenciales, promoverá la cultura de prevención y cumplimiento normativo, y adoptará medidas administrativas, disciplinarias, contractuales o legales frente al incumplimiento de los lineamientos establecidos en la presente política, en articulación con el SIGRIP, el PTEP y el Sistema Integrado de Gestión.

5.1.3 Política Antisoborno

El Ministerio de Igualdad y Equidad adopta la presente Política Antisoborno con el propósito de prevenir, detectar y rechazar cualquier forma de soborno, beneficio indebido, dádiva, pago irregular, favor o práctica corrupta que pueda afectar la transparencia, la integridad institucional, la adecuada gestión pública o la confianza ciudadana.

Todas, todos y todes las, los y les servidores públicos, contratistas, directivos, firmas proveedoras y demás personas o terceras partes vinculadas a la gestión institucional deberán actuar conforme a los mandatos rectores de transparencia, ética pública, legalidad y responsabilidad, absteniéndose de ofrecer, prometer, solicitar, autorizar o recibir beneficios indebidos en el desarrollo de sus funciones o actividades relacionadas con el Ministerio.

El Ministerio fortalecerá los mecanismos de prevención y control mediante la implementación de procesos de debida diligencia, monitoreo de riesgos, canales de denuncia protegidos, acciones de sensibilización y seguimiento permanente a señales de alerta asociadas a riesgos de soborno, en articulación con el SIGRIP, el Programa de Transparencia y Ética Pública (PTEP) y la normatividad colombiana vigente en materia de lucha contra la corrupción.

El incumplimiento de los lineamientos establecidos en la presente política dará lugar a

las acciones administrativas, disciplinarias, fiscales, contractuales y penales correspondientes, conforme a la normatividad vigente.

5.1.4 Política Antifraude

El Ministerio de Igualdad y Equidad adopta la Política Antifraude con el propósito de prevenir, detectar, controlar y gestionar conductas fraudulentas, actos de corrupción, manipulación de información, uso indebido de recursos públicos y cualquier otra actuación irregular que pueda afectar la integridad institucional, la transparencia, la confianza ciudadana o el cumplimiento de los objetivos estratégicos y misionales de la Entidad. Para ello, promoverá una cultura institucional basada en la ética pública, la legalidad, el autocontrol y la responsabilidad en el ejercicio de las funciones públicas, a cargo de todas, todos y todes las, los y les servidores públicos, contratistas y personal vinculado.

La Entidad implementará mecanismos preventivos y de control orientados al fortalecimiento de la gestión del riesgo, la debida diligencia, los canales de denuncia, el monitoreo de señales de alerta y la adopción de medidas correctivas y disciplinarias frente a posibles situaciones de fraude, en articulación con el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), el Programa de Transparencia y Ética Pública (PTEP), el Modelo Integrado de Planeación y Gestión (MIPG) y la normatividad colombiana vigente en materia de integridad pública, control interno y lucha contra la corrupción.

5.2 Lineamiento con relación a la política

5.2.1 Gobierno de riesgos

El Equipo Directivo del Ministerio de Igualdad y Equidad asume el compromiso de fortalecer y mantener una estructura organizacional adecuada que soporte la implementación, sostenibilidad y mejora continua del tema Integrado de Gestión de Riesgos e Integridad Pública (SIGRIP), promoviendo el seguimiento permanente al nivel de madurez, efectividad de los controles y capacidad institucional para la gestión preventiva de los riesgos.

La gestión integral del riesgo se desarrollará en articulación con el Modelo Integrado de

Planeación y Gestión (MIPG) y el Modelo Estándar de Control Interno (MECI), promoviendo un enfoque preventivo, sistemático y transversal orientado al fortalecimiento del control interno, la transparencia, la integridad pública y el cumplimiento de los objetivos institucionales.

La Alta Dirección define un nivel de apetito al riesgo bajo para los riesgos asociados a la gestión institucional y establece cero tolerancia frente a riesgos relacionados con corrupción, fraude, soborno, conflicto de intereses, lavado de activos, financiación del terrorismo, financiación de la proliferación de armas de destrucción masiva y demás conductas que afecten la integridad pública. En consecuencia, todos los procesos deberán garantizar la implementación de controles y acciones de tratamiento orientadas a mantener los riesgos residuales dentro de niveles aceptables.

El Ministerio de Igualdad y Equidad reconoce que la gestión integral del riesgo es responsabilidad de todos los servidores públicos, contratistas y terceros que intervienen en el desarrollo de los procesos institucionales. La responsabilidad sobre la identificación, análisis, valoración, tratamiento, monitoreo, seguimiento y reporte de los riesgos recae especialmente en los líderes y dueños de proceso, quienes deberán garantizar la implementación y efectividad de los controles definidos.

Así mismo, el Ministerio promoverá el fortalecimiento de la cultura organizacional orientada a la gestión del riesgo, fomentando el autocontrol, la mejora continua y la toma de decisiones basada en riesgos en todos los niveles institucionales.

La gestión integral del riesgo se desarrollará bajo el esquema de líneas de defensa, conforme a los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG y del Modelo Estándar de Control Interno – MECI, así:

- **Primera Línea de Defensa:** directores, coordinadores, líderes y ejecutores de los procesos, responsables de gestionar los riesgos y ejercer el autocontrol en el desarrollo de las actividades institucionales.
- **Segunda Línea de Defensa:** Oficina Asesora de Planeación y demás dependencias responsables del liderazgo, seguimiento y monitoreo de políticas, subsistemas y controles asociados al Sistema Integrado de Gestión y MIPG.
- **Tercera Línea de Defensa:** Oficina de Control Interno, responsable de realizar evaluación independiente sobre la efectividad de la gestión integral del riesgo y del sistema de control interno institucional.

5.2.2 Cultura de riesgos

Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno dispone de los recursos necesarios para el impulso, fortalecimiento y

mantenimiento de la cultura de gestión de riesgos al interior de todos los procesos del Ministerio incluidas las direcciones territoriales, dando los lineamientos para establecer las herramientas que deben ser implementadas para la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los diferentes tipos de riesgos a los que está expuesta.

Desde la Oficina asesora de planeación se impulsa la gestión unificada de los diferentes tipos de riesgos a nivel de todo el Ministerio, promueve las directrices, herramientas y metodologías para la articulación de los diferentes elementos de administración de riesgos en la cultura corporativa propendiendo por el aseguramiento y control de los procesos.

5.2.3 Apetito, tolerancia y capacidad del riesgo

El Ministerio de Igualdad y Equidad establecerá criterios de apetito y tolerancia al riesgo como mecanismos orientadores para la toma de decisiones, el tratamiento de riesgos y la definición de acciones de monitoreo y control, conforme a la naturaleza, impacto y criticidad de los riesgos identificados.

Los niveles de apetito y tolerancia permitirán determinar el nivel de exposición al riesgo que la entidad está dispuesta a asumir en desarrollo de sus objetivos institucionales, así como las condiciones bajo las cuales deberán adoptarse acciones de tratamiento, mitigación, seguimiento o escalamiento.

La Alta Dirección definirá y revisará periódicamente los niveles de apetito, tolerancia, aceptación y capacidad del riesgo, teniendo en cuenta la naturaleza de los procesos, el impacto potencial sobre los recursos públicos, la prestación del servicio, la seguridad de la información y el cumplimiento de los objetivos institucionales.

Para los riesgos de integridad pública y corrupción, la entidad mantendrá un nivel de tolerancia restrictivo, orientado a la prevención, detección y control permanente de posibles hechos asociados a conductas contrarias a la integridad y la transparencia institucional.

El Ministerio establece un nivel de apetito al riesgo bajo para los riesgos asociados a la gestión institucional y cero tolerancia frente a riesgos relacionados con corrupción, fraude, soborno, conflictos de interés, lavado de activos, financiación del terrorismo, financiación de la proliferación de armas, afectación a la integridad pública y vulneración de la seguridad de la información crítica.

Todos los procesos deberán implementar controles y acciones de tratamiento orientadas a mantener los riesgos residuales dentro de los niveles de aceptación definidos institucionalmente, fortaleciendo el monitoreo, seguimiento y mejora continua del Sistema Integral de Gestión del Riesgo.

De manera general, se establecen los siguientes criterios institucionales de actuación:

Nivel de Riesgo Residual	Nivel de Tolerancia	Criterio General de Actuación
Bajo	Aceptable	El riesgo podrá mantenerse bajo monitoreo periódico y controles existentes.
Moderado	Tolerancia controlada	Requiere seguimiento y fortalecimiento de controles cuando se identifiquen desviaciones relevantes.
Alto	Tolerancia restringida	Requiere implementación prioritaria de acciones de tratamiento y seguimiento reforzado.
Extremo	No aceptable	Requiere intervención inmediata, escalamiento y definición de acciones correctivas prioritarias.

La entidad podrá establecer criterios específicos de tolerancia y monitoreo para determinados tipos de riesgo conforme a su criticidad, impacto institucional y obligaciones normativas aplicables.

Cuando un riesgo residual supere los niveles de tolerancia definidos por la entidad o presente incremento significativo en su nivel de exposición, deberán adoptarse medidas de análisis, tratamiento y escalamiento conforme a la criticidad del riesgo identificado.

En estos casos, los líderes de proceso y responsables de riesgo deberán:

- Informar oportunamente a la segunda línea de defensa.
- Evaluar la efectividad de los controles existentes.
- Definir e implementar acciones de tratamiento adicionales.
- Fortalecer las actividades de monitoreo y seguimiento.
- Reportar los avances y resultados de las acciones implementadas.

Los riesgos clasificados en nivel alto o extremo podrán ser presentados ante las instancias institucionales competentes para la toma de decisiones, priorización de acciones o definición de medidas adicionales de control.

5.3 Cumplimiento de normatividad interna y externa relacionadas con la administración de riesgos

El modelo integrado e planeación y gestión (MIPG) define para su operación articulada la creación del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

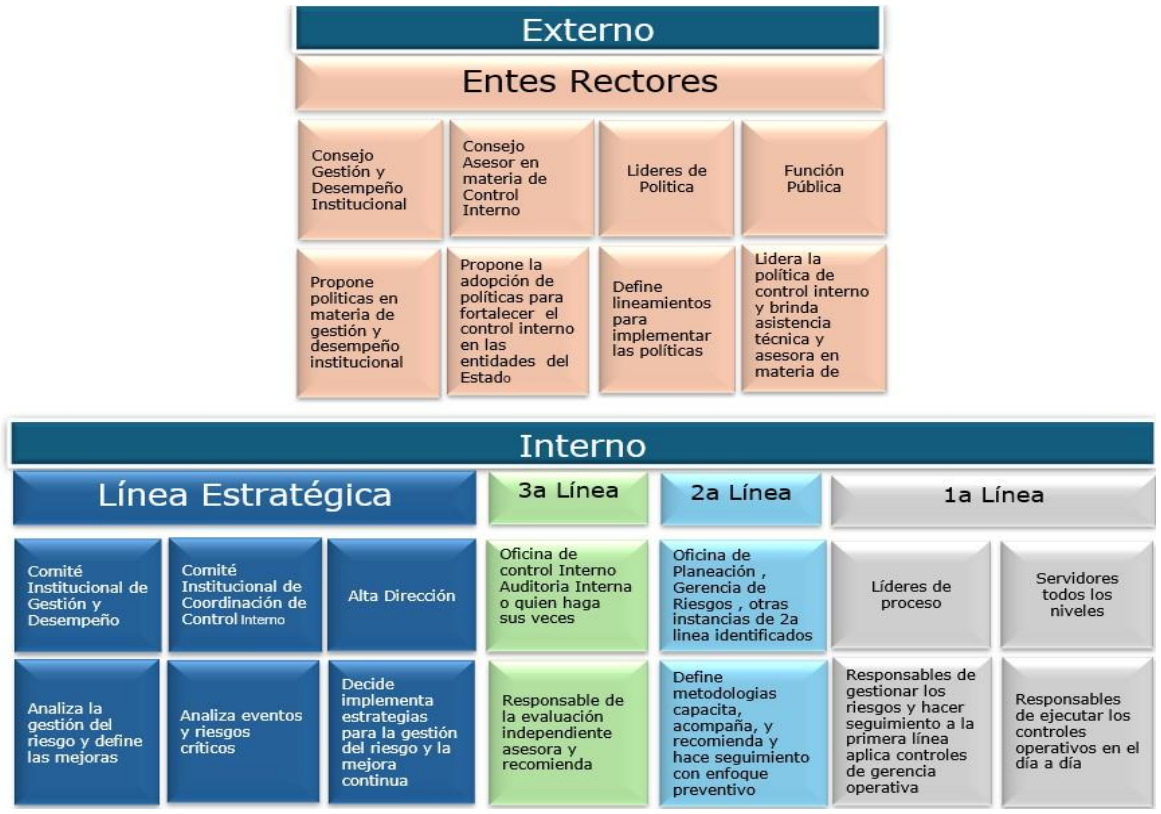


Tabla 1 Institucionalidad del MIPG desde la perspectiva de gestión del riesgo
Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

El Comité Institucional de Gestión y Desempeño es un órgano rector como supervisor, que asegura que la entidad tenga un enfoque integral, sistemático y sostenible para identificar, controlar y gestionar los riesgos que puedan afectar el cumplimiento de sus objetivos estratégicos y de procesos tomando como referencia los diferentes marcos y

estándares normativos que enmarcan a los sistemas de administración de riesgos entre estos: Estatuto anticorrupción ley 1474 de 2011, COSO ERM, Modelo Estándar de Planeación y Gestión, MECI

El Comité Institucional de Coordinación de Control Interno como Línea Estratégica (Alta Dirección) debe definir y aprobar la Política de Administración del Riesgo, atender la periodicidad para el seguimiento a riesgos críticos haciendo uso de la información suministrada por las instancias de 2ª línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, riesgos materializados retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.

El Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo Estándar de Control Interno (MECI), ambos adoptados mediante el Decreto 1499 de 2017 y el Decreto 1083 de 2015 (modificado), establecen que la gestión de riesgos es un componente transversal de los sistemas de gestión pública. El dominio de control del MECI enfatiza la importancia del "Ambiente de Control", dentro del cual el tono desde la cima representa la base para la implementación efectiva del control interno, incluyendo la prevención del fraude, la corrupción y otras prácticas indebidas. **(Guía para la Gestión Integral del Riesgo en Entidades Públicas, 2025 V7, pág. 28)**.

La Política de Administración de Riesgos establece las directrices vinculantes para todas las dependencias del Ministerio, las direcciones territoriales y las áreas que ejecutan procesos tercerizados, en concordancia con la estructura ministerial definida en el Decreto 1075 de 2024. Estas políticas son de obligatorio cumplimiento y su implementación debe ser supervisada y documentada por todos los servidores públicos, contratistas y terceros que participen en los procesos institucionales, garantizando así una gestión integral y estandarizada de los riesgos en todos los niveles de la organización.

6. PROCESO DE GESTIÓN DE RIESGOS

6.1 Metodología para la gestión de riesgos

El Ministerio de Igualdad y Equidad adoptará la metodología general para la gestión integral del riesgo establecida por el Departamento Administrativo de la Función Pública (DAFP), articulada con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo Estándar de Control Interno (MECI) y el Sistema Integrado de Gestión de Riesgos e Integridad Pública (SIGRIP). El proceso se desarrollará a través de los siguientes componentes y pasos obligatorios:

- **Análisis del contexto interno y externo:** Fase preliminar y estratégica donde se definen los límites del sistema, se caracteriza la realidad institucional y territorial del Ministerio (mediante un análisis multidimensional) y se establece la Política de Gestión Integral del Riesgo como base técnica para la toma de decisiones.
- **Identificación y descripción del riesgo:** Etapa orientada a realizar la identificación de los puntos de riesgo, la identificación de áreas de impacto, la identificación de áreas de factores de riesgo y la descripción detallada del riesgo.
- **Análisis de Riesgo Inherente:** Proceso técnico enfocado en determinar la probabilidad y determinar el impacto de los eventos identificados, con el fin de realizar el correspondiente análisis de severidad sin considerar la presencia de medidas de mitigación.
- **Diseño y Análisis de Controles:** Fase en la cual se establece la estructura para la descripción del control y se efectúa la valoración cualitativa o cuantitativa de los controles existentes en la Entidad.
- **Valoración de Riesgo Residual:** Etapa donde se realiza la aplicación de la efectividad de los controles, se evalúa su desplazamiento en la matriz de severidad y se consolida el Mapa de Riesgos definitivo.
- **Monitoreo y Revisión:** Componente transversal y continuo que retroalimenta de manera permanente a todo el sistema, garantizando la supervisión constante de las etapas y la actualización oportuna de las herramientas de gestión.

La aplicación de cada una de las fases de este esquema metodológico será de obligatorio cumplimiento para todas las dependencias y requerirá el compromiso activo de todas, todos y todes personas en servidores públicos, directivos, contratistas y terceras partes vinculadas a la gestión institucional del Ministerio.

Ilustración 1. Metodología general para la gestión integral del riesgo

Fuente: Capacitación DAFP (2 oct 2025) Guía para la gestión integral de riesgos DAFP-2025 V.7

6.2 Análisis del Contexto Interno y externo

El Ministerio de Igualdad y Equidad establecerá, formalizará y mantendrá actualizado el contexto estratégico institucional como la fase inicial y base obligatoria del **Sistema Integrado de Gestión de Riesgos e Integridad Pública (SIGRIP)**. Este análisis tiene como propósito caracterizar de forma real y medible los factores internos y externos que puedan impactar positiva o negativamente el cumplimiento de los objetivos institucionales, la prestación de los servicios, la protección de los recursos públicos y la generación de valor público.

Para la determinación, formalización y estandarización de este contexto, los líderes de proceso, en conjunto con sus respectivos enlaces estratégicos y bajo la orientación de la Oficina Asesora de Planeación y la Función de Cumplimiento, deberán diligenciar obligatoriamente el **Plantilla Matriz de Riesgos Institucional (Código: GE-A-FO-005)**, aplicando la siguiente estructura metodológica y operativa:

A. Análisis Multidimensional del Entorno (Matriz DOFA por Dimensiones) El proceso evaluará de manera simultánea sus capacidades internas (Fortalezas y Debilidades) y las variables del entorno externo (Oportunidades y Amenazas)

cruzándolas de forma obligatoria a través de cinco (5) dimensiones técnicas:

1. **Dimensión Política y Normativa:** Análisis de las políticas de gobierno, prioridades del Plan Nacional de Desarrollo, asignación y comportamiento del Presupuesto General de la Nación, junto con las leyes, decretos, jurisprudencia y mandatos constitucionales vigentes que rigen el objeto misional del proceso.
2. **Dimensión Técnica y Operativa:** Evaluación de la madurez del Sistema Integrado de Gestión (SIG), la interrelación e integración de los subprocesos, la capacidad e infraestructura física instalada, la asignación de responsabilidades y la efectividad de las salvaguardas y controles operativos existentes.
3. **Dimensión Económica y Financiera:** Diagnóstico del presupuesto institucional asignado al proceso, capacidad de ejecución presupuestal, flujos de recursos, costos de operación y variables socioeconómicas del país que impacten la viabilidad financiera de los programas del Ministerio.
4. **Dimensión Social y Comunitaria:** Caracterización de las dinámicas culturales, brechas de desigualdad, necesidades demográficas, y el nivel de relacionamiento y expectativas de los grupos de valor, beneficiarios, contratistas, operadores y comunidades del territorio donde interviene el proceso.
5. **Dimensión Tecnológica y de Inversión:** Evaluación de las herramientas de software disponibles, plataformas de datos, infraestructura de red, capacidades de ciberseguridad, nivel de automatización de trámites y apropiación de la innovación tecnológica.

B. Consolidación de la Matriz DOFA General Con base en la identificación multidimensional previa, cada líder de proceso consolidará los factores críticos detectados en la estructura general de la **Matriz DOFA**, clasificándolos estrictamente bajo los siguientes criterios técnicos:

- **Fortalezas (F):** Capacidades internas positivas y recursos propios que facilitan el logro de los objetivos del proceso.
- **Debilidades (D):** Factores internos negativos, fallas de gestión, recursos insuficientes o limitaciones que restringen el desempeño del proceso.
- **Oportunidades (O):** Factores externos positivos del entorno que pueden ser aprovechados para potenciar la mejora del desempeño institucional.
- **Amenazas (A):** Factores externos negativos que podrían poner en riesgo la continuidad del proceso si no se gestionan adecuadamente.

C. Análisis Estratégico y Formulación de Estrategias Cruzadas El ejercicio de contexto no se limitará a un listado de factores. Cada proceso deberá realizar obligatoriamente el cruce estratégico de variables para definir los planes de acción institucionales que servirán de insumo directo para formular las causas de los riesgos en las tipologías del SIGRIP. Las estrategias se clasificarán de la siguiente manera:

- **Estrategias FO (Ofensivas - Fortalezas + Oportunidades):** Acciones para usar las capacidades internas con el fin de potenciar y aprovechar las oportunidades del entorno.
- **Estrategias DO (Adaptativas - Debilidades + Oportunidades):** Acciones orientadas a superar las debilidades internas del proceso aprovechando las ventajas externas identificadas.
- **Estrategias FA (Defensivas - Fortalezas + Amenazas):** Acciones destinadas a utilizar las fortalezas del proceso para mitigar, reducir o evadir el impacto de las amenazas externas.
- **Estrategias DA (Supervivencia o Contingencia - Debilidades + Amenazas):** Acciones críticas enfocadas a contrarrestar las debilidades internas y blindar al proceso frente a las amenazas del entorno, previniendo su parálisis operativa.

Las estrategias resultantes de los cuadrantes **FA** y **DA** serán prioritarias y de uso obligatorio para la identificación de causas de riesgos de *Gestión, Integridad Pública (corrupción, fraude, soborno, conflictos de interés), Seguridad de la Información, Riesgos Fiscales y LA/FT/FP*.

D. Periodicidad, Actualización y Grupos de Valor

- El **Formato de Análisis del Contexto por Proceso** deberá ser diligenciado, revisado y actualizado anualmente por todos los procesos del Ministerio durante el primer trimestre de cada vigencia.
- Se generará una actualización extraordinaria e inmediata de este análisis cuando ocurran cambios significativos en la estructura orgánica del Ministerio, reformas normativas que alteren sus competencias, variaciones drásticas en el presupuesto asignado, crisis del entorno social o territorial, o modificaciones estructurales en el modelo de operación institucional.
- En todo el proceso de análisis multidimensional se deberán incorporar formalmente las necesidades, expectativas y alertas tempranas manifestadas por

los grupos de valor, beneficiarios, contratistas, operadores y la ciudadanía en general, asegurando que el mapa de riesgos refleje la realidad territorial de las poblaciones atendidas, en estricta concordancia con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Versión 7 de 2025 del DAFP.

D. Identificación de los puntos críticos: Para la identificación de los riesgos de proceso, se debe tener en cuenta las actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo. Es importante que se analice la secuencia de los procesos y la cadena de valor, lo cual permite identificar los puntos críticos y el establecimiento de las actividades que pueden generar riesgo para el cumplimiento de los objetivos de los procesos de la Entidad. (mapa de procesos)

E. Identificación de las áreas de impacto: De conformidad con la metodología establecida por el DAFP, se debe identificar las áreas de impacto, estas son: "la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional."

F. Identificación de las áreas de factores de riesgos: Estas hacen referencia a la identificación de las fuentes generadoras de riesgos que pueda tener la Entidad, a nivel interno y externo.

6.3 Esquema para la Gestión de riesgos de seguridad de la información

La metodología para la gestión de los riesgos de Seguridad de la información se basa en la metodología establecida en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC y la Guía para la gestión Integral del riesgo en Entidades Públicas Versión 7.

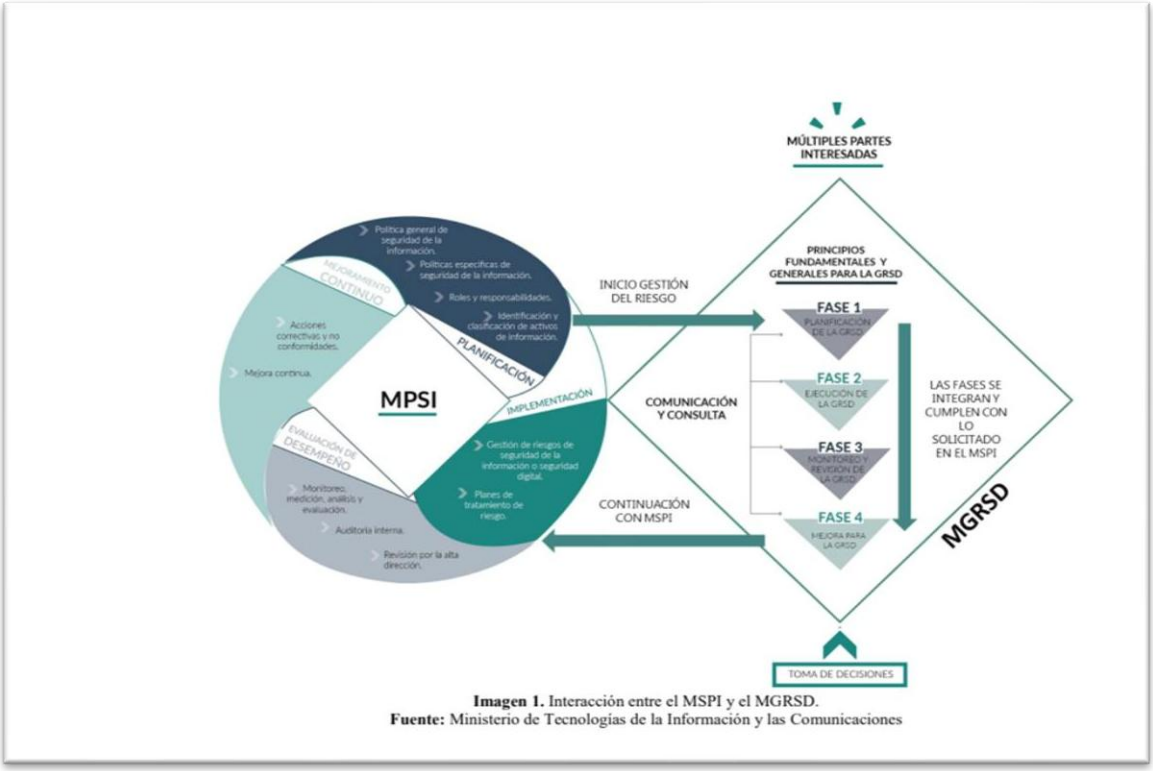


Imagen 1. Interacción entre el MSPI y el MGRSD.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Ilustración 2 Administración de riesgos digitales
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

6.4 Identificación y descripción del riesgos emergentes

La identificación y descripción de riesgos emergentes consiste en reconocer, analizar y documentar aquellos riesgos nuevos, cambiantes o en evolución que pueden afectar el cumplimiento de los objetivos institucionales, como consecuencia de transformaciones tecnológicas, sociales, ambientales, económicas, regulatorias o políticas, y cuya probabilidad e impacto pueden ser inciertos o difíciles de anticipar debido a la dinámica del entorno.

En este sentido, el Ministerio de Igualdad y Equidad fortalecerá la implementación de análisis prospectivos y herramientas de monitoreo orientadas a una gestión preventiva, dinámica y articulada de los riesgos emergentes, mediante la aplicación de los siguientes lineamientos:

- Realizar ejercicios de vigilancia tecnológica, análisis de tendencias, y construcción de escenarios.
- Incorporar el análisis de riesgos emergentes en los espacios de planeación estratégica.

- Revisar periódicamente fuentes externas (OCDE, DAFP, organismos multilaterales).
- Integrar estos riesgos en mapas de riesgo dinámicos con seguimiento periódico.

7. HERRAMIENTA PARA GESTION DEL RIESGO

El Ministerio de Igualdad y Equidad adopta metodología suministrada por el DAFP de conformidad con el esquema para la gestión de riesgos.

De acuerdo con lo anterior, el formato de mapa de riesgos de gestión adoptado por la entidad se encuentra controlado con el formato **GE_A-FO-005** para la identificación; análisis; evaluación de riesgos y valoración de controles; evaluación del riesgo residual; planes de manejo con sus respectivos campos, para los riesgos de gestión, fiscal y de corrupción.

Para la gestión de los riesgos de Seguridad de la Información, se estructuró la matriz para la identificación y el análisis de los riesgos inherentes; valoración de los controles y planes de manejo con sus respectivos campos con el formato TI_S**-FO-003**, bajo los parámetros de la Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7.

Los formatos para la gestión de riesgos se deben diligenciar acorde con el instructivo que contiene cada formato.

7.1 Mapa de riesgos

El mapa de riesgos es una herramienta visual de gestión que permite identificar, evaluar y priorizar los riesgos a los que está expuesta una organización, proyecto o proceso. Su elaboración estará a cargo de cada uno de los líderes de proceso y será consolidado por la Oficina Asesora de Planeación. Este instrumento integrará los riesgos de gestión, fiscales, de seguridad de la información y de corrupción asociados a cada proceso.

El mapa de riesgos Institucional GE_A-FO-006

Es consolidado por la Oficina de Planeación y estará conformado por los riesgos

residuales, que se encuentren en una zona de riesgo, moderada, alta o extrema de los riesgos de gestión, fiscales y de corrupción.

El mapa de riesgo Institucional recopila los planes de manejo de los riesgos de cada proceso y los cuales son susceptibles de seguimiento por parte de la Oficina Asesora de Planeación y de Control Interno.
La Oficina Asesora de Planeación, publicará los mapas de riesgos, en la página web de la Entidad, en el enlace de transparencia, de acuerdo con lo establecido en la Ley 1712 de 2014 y el Decreto 103 de 2015 y la Ley 1474 de 2011.

7.1.1 Importancia de la Gestión de Riesgos

Permite identificar de manera oportuna los eventos potenciales tanto internos como externos que puedan afectar el cumplimiento de los objetivos y misión institucional.
Evita que los eventos negativos, lesionen la imagen institucional, entorpezcan la operación, el cumplimiento de los objetivos estratégicos y metas institucionales o que afecten la prestación de los servicios.

Permite, controlar y dar tratamiento prioritario a los riesgos de gestión y de seguridad digital de mayor incidencia y los relacionados con los riesgos de corrupción.
Potencializa los eventos positivos, para que permitan minimizar el impacto de los posibles eventos negativos en la gestión de los riesgos.

Identifica, disuade y detecta posibles fraudes que puedan afectar la adecuada gestión de la Entidad.

Incrementa la confianza de todos los procesos del Ministerio en el uso del entorno digital.
Asegura que los datos, sistemas de información e infraestructura tecnológica estén protegidos contra amenazas.

7.2 Apetito al riesgo

En cumplimiento de los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 de 2025, el Ministerio de Igualdad y Equidad

establecerá criterios para la determinación, análisis, monitoreo y revisión del apetito, tolerancia y capacidad del riesgo, como elementos orientadores para la toma de decisiones institucionales y la gestión preventiva de los riesgos asociados al cumplimiento de los objetivos estratégicos, misionales y operativos de la Entidad.

Para efectos de la presente política, se adoptan las siguientes definiciones:

- **Nivel de riesgo:** corresponde al valor resultante de combinar la probabilidad de ocurrencia de un evento con el impacto que este podría generar sobre el cumplimiento de los objetivos institucionales, la prestación de los servicios, la integridad pública, los recursos públicos o la gestión institucional.
- **Apetito al riesgo:** corresponde al nivel de riesgo que el Ministerio está dispuesto a aceptar o asumir en el desarrollo de sus actividades y objetivos institucionales, de conformidad con el marco legal, la capacidad institucional y las directrices definidas por la Alta Dirección.
- **Tolerancia del riesgo:** corresponde al nivel máximo de desviación aceptable respecto al apetito de riesgo definido por la Entidad, a partir del cual deberán implementarse acciones de tratamiento, seguimiento reforzado o escalamiento institucional.
- **Capacidad de riesgo:** corresponde al nivel máximo de riesgo que el Ministerio puede soportar sin afectar de manera significativa el cumplimiento de sus objetivos estratégicos, la continuidad institucional, la prestación del servicio o la adecuada administración de los recursos públicos.

El Ministerio establecerá criterios diferenciales para la gestión del apetito y tolerancia del riesgo, considerando la naturaleza y criticidad de cada tipología de riesgo. En este sentido:

- Los riesgos asociados a integridad pública, corrupción, fraude, soborno y LA/FT/FP tendrán un nivel de apetito bajo o cero tolerancia, dada su afectación potencial sobre la legalidad, la transparencia y la confianza institucional.
- Los riesgos fiscales tendrán tolerancia mínima, considerando su posible impacto sobre los recursos públicos y el patrimonio del Estado.

- Los riesgos de seguridad de la información deberán mantenerse dentro de niveles controlados y aceptables conforme a criterios de confidencialidad, integridad y disponibilidad.
- Los riesgos de gestión podrán admitir niveles moderados de tolerancia, siempre que existan controles, monitoreo y acciones de tratamiento que permitan mantenerlos dentro de niveles aceptables para la Entidad.

La definición, revisión y aprobación de los niveles de apetito, tolerancia y capacidad del riesgo será responsabilidad de la Alta Dirección y del Comité Institucional de Coordinación de Control Interno, con el apoyo técnico de la Oficina Asesora de Planeación como segunda línea de defensa. Estos criterios deberán revisarse como mínimo una vez al año o cuando se presenten cambios significativos en el contexto institucional, normativo, operativo o estratégico del Ministerio.

Cuando un riesgo residual supere los niveles de tolerancia definidos por la Entidad, el líder del proceso correspondiente deberá implementar acciones inmediatas de tratamiento y reportar la situación a la segunda línea de defensa para su análisis y seguimiento. En caso de que el riesgo alcance niveles críticos o supere la capacidad institucional definida, la situación deberá escalarse a la Alta Dirección y al Comité Institucional de Coordinación de Control Interno para la toma de decisiones y definición de medidas adicionales de control, mitigación o contingencia.

La siguiente ilustración presenta la relación conceptual entre la capacidad, la tolerancia y el apetito del riesgo, como elementos orientadores para la gestión institucional y la toma de decisiones frente a la exposición a los diferentes tipos de riesgos asociados a los procesos, proyectos, trámites y actividades del Ministerio de Igualdad y Equidad, tales como riesgos de gestión, integridad pública, corrupción, fraude, soborno, conflictos de interés, LA/FT/FP, riesgos fiscales y riesgos de seguridad de la información.

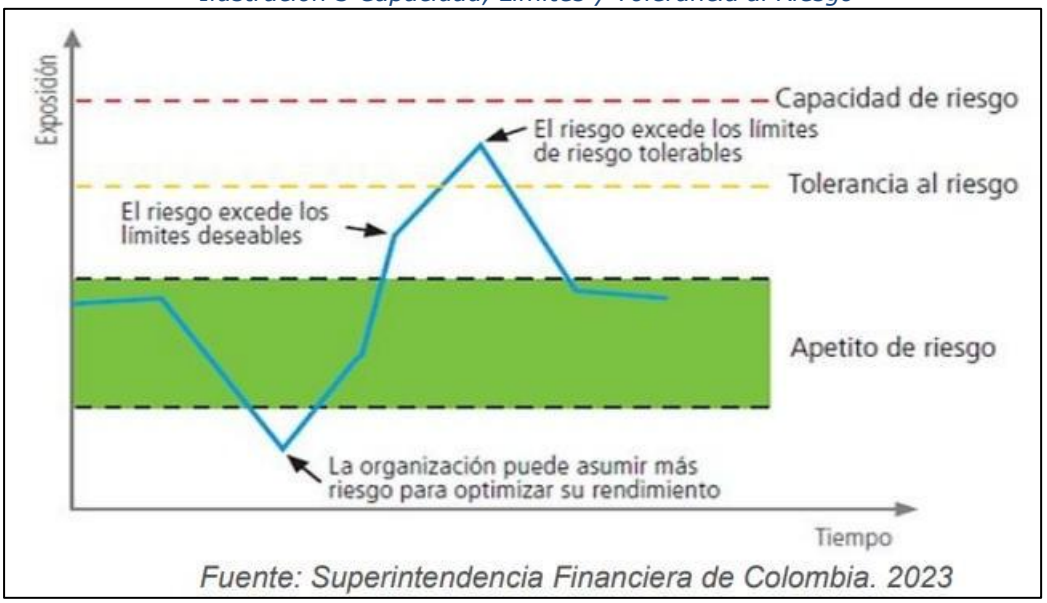
Capacidad de Riesgo (línea roja superior): Corresponde al nivel máximo de riesgo que la Entidad puede soportar sin comprometer el cumplimiento de sus objetivos estratégicos, la continuidad institucional, la prestación de los servicios, la integridad pública o la adecuada administración de los recursos públicos. Este límite no debe ser

superado en ninguna circunstancia, especialmente en riesgos asociados a corrupción, fraude, soborno, LA/FT/FP y riesgos fiscales.

Tolerancia del Riesgo (línea intermedia): Corresponde al nivel máximo de desviación aceptable respecto al apetito del riesgo definido por la Entidad. Este nivel actúa como un umbral de control y seguimiento, a partir del cual deberán implementarse acciones de tratamiento, monitoreo reforzado, fortalecimiento de controles y mecanismos de escalamiento institucional, según la naturaleza y criticidad de cada tipología de riesgo.

Apetito de Riesgo (línea variable): Corresponde al nivel de riesgo que el Ministerio está dispuesto a asumir para el cumplimiento de sus objetivos institucionales, considerando el contexto estratégico, la capacidad institucional, el marco normativo, los controles existentes y las directrices definidas por la Alta Dirección. El nivel de apetito podrá variar según el tipo de riesgo, estableciendo niveles bajos o de cero tolerancia para riesgos relacionados con integridad pública, corrupción, fraude, soborno y LA/FT/FP, y niveles moderados o controlados para riesgos operativos, estratégicos y administrativos, siempre que existan mecanismos adecuados de control y seguimiento.

Ilustración 3 Capacidad, Límites y Tolerancia al Riesgo



Fuente: Citado en Guía para la gestión integral de riesgos DAFP-2025 V.7

La gráfica demuestra que, aunque el riesgo real (línea azul) varía considerablemente

durante el proceso, siempre debe mantenerse dentro de los límites establecidos por la tolerancia (amarillo) y nunca exceder la capacidad (roja).

7.3 Tolerancia de los riesgos

De acuerdo con la calificación de los riesgos residuales obtenidos tras la valoración de los controles, el Ministerio de Igualdad y Equidad establece la tolerancia, los criterios de respuesta y las opciones de tratamiento obligatorias para los factores de gestión, seguridad digital, fiscales y de integridad pública:

- **Riesgos de Gestión y Seguridad Digital:** Sus niveles de tolerancia admitirán desviaciones moderadas y sus opciones de tratamiento incluirán, según el análisis de viabilidad de cada líder de proceso, las acciones de reducir, evitar, compartir, aceptar o transferir el riesgo.
- **Riesgos para la Integridad Pública y Fiscales:** Estas tipologías —que abarcan actos de corrupción, fraude, soborno, conflicto de intereses, así como el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP)— son catalogadas como inaceptables para la administración.
- **Restricciones de Tratamiento:** Por su naturaleza crítica, los riesgos para la integridad pública y fiscales no admiten en ninguna circunstancia las opciones de aceptación, compartición o transferencia del riesgo. Su tratamiento es imperativo y obligatorio, sin importar la calificación final del riesgo residual, enfocándose únicamente en implementar acciones directas para **evitar o reducir** el riesgo mediante el bloqueo de sus causas.

7.4 Niveles de aceptación al riesgo

Los niveles de aceptación del riesgo se determinan como resultado de la valoración de la probabilidad de ocurrencia del riesgo y de la magnitud del impacto al momento de evaluar su materialización. Los riesgos de gestión inherentes, ubicados en la zona de riesgos “baja” pueden ser aceptados y por lo tanto no es necesario establecer controles. Los riesgos de corrupción son los únicos que son inaceptables en todo sentido, por tanto, deben tener controles permanentes y realizar su seguimiento.

El mapa de calor de riesgos permite visualizar los riesgos de gestión en las zonas de riesgos definidas (Baja, Moderada, Alta, Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a buscar o retener (apetito del riesgo) en función del impacto de estos en el Ministerio. Los riesgos que se encuentren en zona baja se aceptan, aunque representan una menor probabilidad e impacto para el Ministerio de Igualdad y Equidad, requieren un seguimiento estructurado que garantice que se mantengan en este nivel. Su monitoreo, si bien puede ser menos intensivo que el de riesgos en zonas más altas, debe ser sistemático y documentado.

Deberá ser:

- Monitoreo trimestral por primera línea
- Revisión cuatrimestral por segunda línea
- Evaluación semestral por control interno
- Actualización de valoración cuando se requiera
- Verificación ante cambios significativos
- Mantención del nivel de riesgo

El mapa de calor de riesgos permite visualizar los riesgos de seguridad digital en las zonas de riesgos definidas (Bajo, Moderado, Alto, Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención; estableciendo un plan de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociado a los activos de información sin importar el nivel de criticidad que tienen para la entidad. Los riesgos de seguridad digital que se encuentren en las zonas Bajo se aceptan, aunque representan una menor probabilidad e impacto, requieren el mimo seguimiento que los riesgos de gestión de zona baja:

- Monitoreo trimestral por primera línea
- Revisión semestral por segunda línea
- Evaluación semestral por control interno
- Actualización de valoración cuando se requiera

- Verificación ante cambios significativos
- Mantención del nivel de riesgo

La Línea Estratégica, debe asegurar una gestión adecuada de los riesgos ubicados en zona baja, garantizando que su tratamiento sea proporcional y eficiente, sin descuidar su monitoreo y control, teniendo en cuenta los siguientes aspectos:

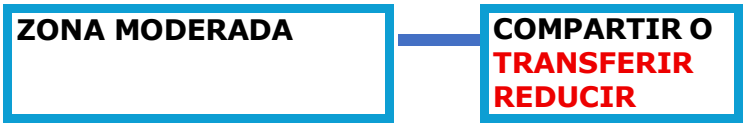
- Validación semestral de informes consolidados
- Evaluación de estrategia de tratamiento
- Toma de decisiones sobre ajustes requeridos
- Definir información requerida
- Determinar indicadores clave
- Aprobar metodología de seguimiento
- Establecer canales de comunicación
- Mantener supervisión adecuada

Los riesgos de corrupción no admiten la aceptación del riesgo, siempre deben conducir a un tratamiento. Los riesgos que se encuentran en las zonas más altas son los que se priorizan orientando los esfuerzos y acciones para mejorar su administración de riesgos.

7.5 Riesgos de gestión y de seguridad de la información

1. 

Asumir (aceptar) la presencia de un riesgo mínimo o residual después de que el riesgo se ha reducido.



Medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas de protección). Se puede conseguir mediante la optimización de los procedimientos y la implementación de controles preventivos.

ZONA ALTA	**EVITAR, COMPARTIR O TRANSFERIR**

Medida encaminada a eliminar la actividad que genera el riesgo (probabilidad y/o impacto), previniendo su materialización.

ZONA EXTREMA	**EVITAR, COMPARTIR O TRANSFERIR**

Medidas que reducen el efecto de un riesgo, a través del traspaso de las pérdidas a otras organizaciones. Y se establecen planes de contingencia en caso de materialización.

7.6 Riesgos de Seguridad de la Información

En coherencia con el Modelo de Seguridad y Privacidad de la Información (MSPI), el Ministerio garantiza la protección de sus activos digitales e información institucional a través de:

- La identificación de activos de información críticos y la valoración de amenazas asociadas.
- La implementación de controles técnicos, administrativos y culturales para salvaguardar la confidencialidad, integridad y disponibilidad de los datos institucionales, así como su privacidad.
- El fortalecimiento de la cultura digital y la formación continua del personal en gestión de incidentes, y prevención de brechas de seguridad.
- El monitoreo y reporte de incidentes conforme a los lineamientos técnicos: en temas de Seguridad de la información; Ciberseguridad; Privacidad de la información.

7.7 Riesgos de Integridad Pública

Los riesgos de integridad pública, entendidos como aquellos que afectan la legalidad, imparcialidad, transparencia y confianza en la gestión pública, incluyen tipologías como corrupción, fraude, soborno, conflicto de interés, así como los riesgos asociados al Lavado de Activos, la Financiación del Terrorismo y la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM), conforme a los lineamientos del Departamento Administrativo de la Función Pública (DAFP), la Ley 2195 de 2022, el Decreto 1122 de 2024 y el Programa

de Transparencia y Ética Pública.

El Ministerio implementa:

- Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas (ALA/CFT/CFP)
- Política Antisoborno
- Política Antifraude
- Procedimiento para gestión de conflictos de interés
- Procedimiento para reporte de operaciones sospechosas
- Canal institucional de denuncias y buzón ético

Articulación Institucional

- Coordinación con órganos de control (Contraloría, Procuraduría, Fiscalía)
- Articulación con la Secretaría de Transparencia de la Presidencia
- Intercambio de información con la UIAF

Teniendo en cuenta el Plan Estratégico de la entidad encontramos varios puntos que presentan mayor susceptibilidad a riesgos de corrupción entre ellos:

Asignación y Distribución de Recursos:

- La gestión de ayudas y subvenciones para poblaciones vulnerables.
- La distribución de recursos para proyectos comunitarios.
- El manejo de presupuestos para infraestructura en territorios excluidos
- La asignación de recursos para iniciativas económicas y productivas.

Contratación y Alianzas:

- Los procesos de contratación para la infraestructura destinada a cerrar brechas territoriales
- La selección de socios para las "Alianzas Públicas Populares, Comunitarias y

Solidarias"
- La contratación de servicios para los Espacios para la Juntanza

Gestión de Programas Sociales:

- La selección de beneficiarios para programas de apoyo.
- La implementación de iniciativas económicas y productivas.
- La distribución de beneficios en territorios marginados

Coordinación Territorial:

- La articulación con entidades territoriales
- La focalización de programas en territorios específicos.
- La implementación de proyectos en zonas marginadas.

Procesos Administrativos:

- La supervisión de contratos y convenios.

La susceptibilidad a la corrupción en estos procesos se incrementa debido a:

- El manejo de recursos significativos
- La interacción con poblaciones vulnerables
- La dispersión geográfica de las intervenciones.
- La complejidad en la verificación y seguimiento
- La discrecionalidad en la toma de decisiones.
- La presión por resultados rápidos en la implementación de programas

Es fundamental establecer un riguroso sistema de tratamiento y seguimiento a los riesgos de corrupción, el éxito en la prevención de la corrupción dependerá de la rigurosidad en la implementación y seguimiento de estas medidas, así como de la participación activa de todos los actores involucrados.

El control y seguimiento será el definido en el numeral 23 del presente documento Monitoreo de los riesgos y controles.

7.8. Liderazgo del Sistema

Según lo establecido en esta Guía, las entidades en el marco de la formulación de la Política para la Gestión Integral de Riesgos deberán asignar unos niveles de responsabilidad cuando se habla de la institucionalidad que se requiere para una gestión del riesgo, se menciona como esta actividad involucra a toda la organización y lo relaciona con las diferentes líneas de aseguramiento que actúan en desarrollo del Modelo Estándar de Control Interno. Para efectos del SIGRIP, existen unos roles y responsabilidades que deben agregarse a esos niveles de responsabilidad. Se relacionan en función del esquema de líneas y los roles que existen en los Programas de Transparencia y Ética Pública, los cuales se resumen a continuación.

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	**Auditor del Programa**	**Administrador del Programa**	**Ejecutores del Programa**
Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno	Oficina de Control Interno, Auditoría Interno o quien haga sus veces	Dependencia o persona designada por la Alta Dirección	Directivos, líderes de proceso, servidores y colaboradores
Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.	En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP asume la función de cumplimiento	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.

Tabla 2 Roles y responsabilidades SIGRIP
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7. 2025

8. TRATAMIENTO O MANEJO DE LOS RIESGOS

A continuación, se presenta el manejo o tratamiento de los riesgos para el Ministerio, de acuerdo con la calificación después de controles (riesgos residuales), los cuales se

califican en zona de riesgo baja, zona de riesgo moderado, zonal de riesgo alta y zona de riesgo extrema. (La metodología para la valoración de los riesgos, se detalla en el numeral 9.4 del presente documento).

Para los riesgos de Seguridad Digital, de acuerdo con la zona que se califique el riesgo, se establece los niveles y el tratamiento que se debe dar, con el fin de evitar su materialización, reducir la zona del riesgo o eliminar el riesgo.

Se debe realizar en primera medida la identificación de los riesgos de seguridad digital para luego definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los niveles establecidos.

El tratamiento de los riesgos involucra identificar las opciones para tratar los riesgos residuales priorizados, con el fin de optimizar los recursos disponibles y enfocar los esfuerzos institucionales, El Ministerio establece como prioridad el tratamiento de los riesgos de seguridad digital ubicados en las zonas de riesgo altas y extremas.

Calificación del Riesgo	(Niveles de aceptación)	Plan de Manejo o Tratamiento del Riesgo
ZONA BAJA	**ASUMIR O ACEPTAR EL RIESGO**	Riesgos inherentes, no se requiere adoptar medidas para su tratamiento. Realizar monitoreo periódico (trimestral) a los riesgos para que permanezcan en zona baja o se permita eliminar el riesgo.
ZONA MODERADA	**REDUCIR EL RIESGO**	Establecer acciones, medidas que permitan reducir la probabilidad y/o el impacto del riesgo. Monitoreos periódicos, mínimo cada trimestre a los riesgos y controles. Optimizar los procedimientos de seguridad digital establecidos

ZONA ALTA	**EVITAR EL RIESGO COMPARTIR O TRANSFERIR EL RIESGO**	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad y/o el impacto. Monitoreo bimensual a los riesgos y controles. Realizar mantenimiento preventivo a la infraestructura tecnológica.
ZONA EXTREMA		Monitoreo mensual a los controles y riesgos y establecer planes de contingencia en caso de materialización. Realizar Contratos de Mantenimiento correctivo, y de soporte sobre la plataforma tecnológica con proveedores. Establecer Contratos de seguro.

Tabla 3 tratamiento del riesgo
Fuente: Elaboración Propia Minigualdad

8.1 Tratamiento riesgos de Integridad Pública y fiscales

Calificación del Riesgo	(Niveles de aceptación)	Plan de Manejo o Tratamiento del Riesgo
ZONA BAJA		Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad de ocurrencia. Monitoreos periódicos, mínimo cada trimestre a los controles y acciones.
ZONA MODERADA	**REDUCIR EL RIESGO**	
ZONA ALTA	**EVITAR EL RIESGO COMPARTIR O TRANSFERIR EL RIESGO**	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando la probabilidad de ocurrencia. Monitoreos bimensuales o mensuales a los riesgos y los controles. Establecer planes de contingencia para aplicar en caso de materialización.
ZONA EXTREMA		

Tabla 4 tratamiento de riesgos de corrupción y fiscales
Fuente: Ministerio de Igualdad y Equidad

Tratamiento de los riesgos de Integridad Publica

El tratamiento de los riesgos de integridad pública debe realizarse de forma diferenciada según la tipología identificada, considerando su naturaleza, causas frecuentes, actores involucrados y canales de control institucional disponibles. En todos los casos, el enfoque debe ser de tolerancia cero, sin aceptación del riesgo residual, priorizando acciones de

prevención, detección temprana y eliminación de condiciones de riesgo.

Evitar o reducir el riesgo. Estos niveles de aceptación, independiente de la calificación de los riesgos residuales.

Los riesgos de Integridad Pública y fiscales no admiten aceptación, compartir o transferir el riesgo y siempre generan tratamiento.

8.1.1 Debida Diligencia

Es imperativo para el ministerio la implementación de debida diligencia en todas las operaciones que involucren terceros, transacciones significativas, proyectos estratégicos y relaciones comerciales. Este proceso consiste en la investigación exhaustiva y el análisis sistemático que permite identificar, evaluar y mitigar riesgos potenciales antes de la toma de decisiones críticas, acorde con los estipulado en el Manual Debida Diligencia (GE_A-MN-005).

Este mecanismo se regirá bajo los siguientes lineamientos y componentes técnicos:

Responsabilidad y Etapas de Aplicación: La debida diligencia será ejecutada por la dependencia o líder de proceso que origine la relación institucional o contractual, actuando como Primera Línea de Defensa, y contará con la asesoría técnica y supervisión de la función de cumplimiento en la Segunda Línea. Este procedimiento se aplicará de manera obligatoria en las etapas precontractual, de planeación o de selección, y se mantendrá de forma continua durante la ejecución y el seguimiento de la operación.

Fuentes de Información y Consultas Obligatorias: El análisis técnico incluirá la revisión detallada de antecedentes fiscales, disciplinarios, penales y de pérdida de investidura, así como la consulta en listas restrictivas nacionales e internacionales, el Registro Único de Beneficiarios Finales (RUB) y bases de datos financieras o de capacidad reputacional.

Segmentación por Nivel de Riesgo: Las contrapartes y terceras partes se clasificarán mediante un enfoque basado en riesgos en niveles Bajo, Medio o Alto. El nivel de profundidad de la debida diligencia y la periodicidad de su actualización serán

proporcionales a esta segmentación, aplicando medidas reforzadas a las operaciones de mayor exposición.

Protocolo ante Alertas y Toma de Decisiones: Cuando los cruces de información arrojen señales de alerta o hallazgos críticos, el proceso se suspenderá de inmediato y el caso será escalado formalmente ante la función de cumplimiento. La Alta Dirección adoptará las decisiones vinculantes a que haya lugar, las cuales podrán incluir el bloqueo de la transacción, la exclusión del proceso de selección o la respectiva compulsa de copias a las autoridades competentes.

Gobernanza de Datos, Archivo y Confidencialidad: Toda la documentación, soportes y resultados de las investigaciones serán administrados bajo estrictos protocolos de confidencialidad, garantizando el archivo documental protegido y el cumplimiento de la normatividad vigente sobre protección de datos personales y habeas data. Esta información estará disponible para los requerimientos de todas, todos y todes las, los y les servidores públicos y contratistas de las Oficinas de Planeación y Control Interno.

8.1.2 La función de cumplimiento

El propósito de la función de cumplimiento es velar por el funcionamiento efectivo, eficiente y oportuno del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) y del Programa de Transparencia y Ética Pública (PTEP), promoviendo el cumplimiento de sus lineamientos y apoyando a las personas líderes de proceso en la mitigación de los factores de riesgo identificados.
Para garantizar la independencia técnica, la entidad emitirá lineamientos y guías para el desarrollo de esta función bajo las siguientes reglas institucionales:

- **Ubicación Institucional (Segunda Línea de Defensa):** El Ministerio de Igualdad y Equidad designa a la Oficina Asesora de Planeación como la dependencia responsable de la función de cumplimiento. En su calidad de segunda línea de defensa y administradora del programa, contará con reporte directo a la Alta Dirección y dispondrá de los recursos humanos, técnicos y tecnológicos requeridos para el desarrollo de sus funciones, conforme a la disponibilidad

presupuestal de la Entidad. La función de cumplimiento, ejercida por la Oficina Asesora de Planeación, tendrá un enfoque preventivo y de articulación institucional, orientado al diseño de herramientas, consolidación de mapas de riesgos, coordinación del PTEP y análisis de alertas derivadas de los procesos de debida diligencia.

- **Responsabilidades de la Función de Cumplimiento:**
  - Coordinar la formulación, articulación, implementación y seguimiento del SIGRIP y del Programa de Transparencia y Ética Pública (PTEP).
  - Administrar y consolidar los resultados de los procedimientos de debida diligencia, orientando a los procesos en la segmentación y análisis de riesgos asociados a terceros y contrapartes.
  - Analizar de manera reservada las alertas relacionadas con operaciones inusuales, señales de riesgo o conductas contrarias a la integridad pública reportadas por las personas vinculadas a la Entidad.
  - Gestionar, cuando corresponda y conforme a la normatividad vigente, los reportes o remisiones de información ante las autoridades competentes en materia de integridad pública, corrupción, fraude o LA/FT/FP.
- **Periodicidad de Reporte:** La dependencia responsable de la función de cumplimiento presentará informes periódicos de gestión, monitoreo y seguimiento a la Alta Dirección y a las instancias institucionales correspondientes, con una periodicidad mínima trimestral, incluyendo el estado de los riesgos, la efectividad de los controles, las alertas identificadas, las acciones implementadas y el nivel de apropiación de la cultura de integridad, transparencia y legalidad por parte de las personas servidoras públicas, contratistas y demás actores vinculados a la gestión institucional.

- **Diferenciación con la Oficina de Control Interno (OCI):** Por su parte, la Oficina de Control Interno actuará exclusivamente como tercera línea de defensa, desarrollando funciones de evaluación independiente, asesoría y formulación de recomendaciones para el fortalecimiento del sistema, sin intervenir en la administración u operación de los riesgos institucionales.

9. TRATAMIENTO DE RIESGOS MATERIALIZADOS

9.1 Detección y evaluación inicial

Cuando se identifique la materialización de un riesgo, el responsable del proceso deberá realizar de manera inmediata una evaluación integral que incluya:
Dimensión y alcance del evento ocurrido, identificando Impacto generado, Consecuencias directas e indirectas en las operaciones y procesos impactados, afectación a objetivos institucionales y hacer un cálculo preliminar de los recursos humanos, técnicos y financieros si es necesario para el tratamiento

Reporte Materialización de Riesgos

Una vez completada la evaluación, el responsable del proceso deberá diligenciar el formato de reporte materialización de riesgos GE_A-FO-012 y remitir el documento a la Oficina Asesora de Planeación mediante correo electrónico institucional, detallando las evidencias, los roles y las responsabilidades asignadas para la contención.

Seguimiento y Monitoreo Continuo: La Oficina Asesora de Planeación (como Segunda Línea de Defensa), con base en la información recibida, realizará un seguimiento continuo, oportuno y prioritario a las acciones correctivas definidas por la dependencia afectada. Para ello, solicitará de manera periódica las evidencias necesarias para verificar la efectividad real de las medidas implementadas y garantizar una mitigación sostenible que evite la recurrencia del evento.

Notificación al Comité Institucional de Gestión y Desempeño: La información de los riesgos materializados será presentada formalmente ante el Comité Institucional de Gestión y Desempeño en su próxima reunión ordinaria o, si la criticidad del incidente compromete la continuidad del Ministerio, en una sesión extraordinaria convocada para tal fin. La presentación deberá estructurarse bajo los siguientes puntos:

- Descripción detallada del riesgo materializado y sus causas raíz.
- Impacto actual y potencial en el cumplimiento de la misión institucional.

- Acciones de contención inmediatas implementadas por el proceso.

- Estado de avance de las medidas adoptadas y propuesta de plan de acción integral.
- Recursos movilizados, presupuesto requerido y cronograma de actividades.
- Resultados preliminares obtenidos tras la intervención.

Facultades del Comité: El Comité Institucional de Gestión y Desempeño se pronunciará sobre las directrices estratégicas de la Entidad y tendrá la facultad legal de aprobar o ajustar los planes de acción propuestos, autorizar la asignación extraordinaria de recursos, coordinar las estrategias de comunicación externa y ordenar las medidas administrativas necesarias.

Documentación, Registro y Lecciones Aprendidas: Todas las acciones, decisiones y resultados deberán ser documentados rigurosamente, en el nforme de Cierre y Lecciones Aprendidas (ICLA) GE_A-FO-030 creando un registro histórico del incidente. Una vez controlado el evento, se adelantará una evaluación de lecciones aprendidas para actualizar las matrices de riesgos, fortalecer los controles internos que se identificaron como débiles, mejorar los protocolos sectoriales y capacitar de manera obligatoria a todas, todos y todes las, los y les servidores públicos, directivos y contratistas vinculados al proceso.

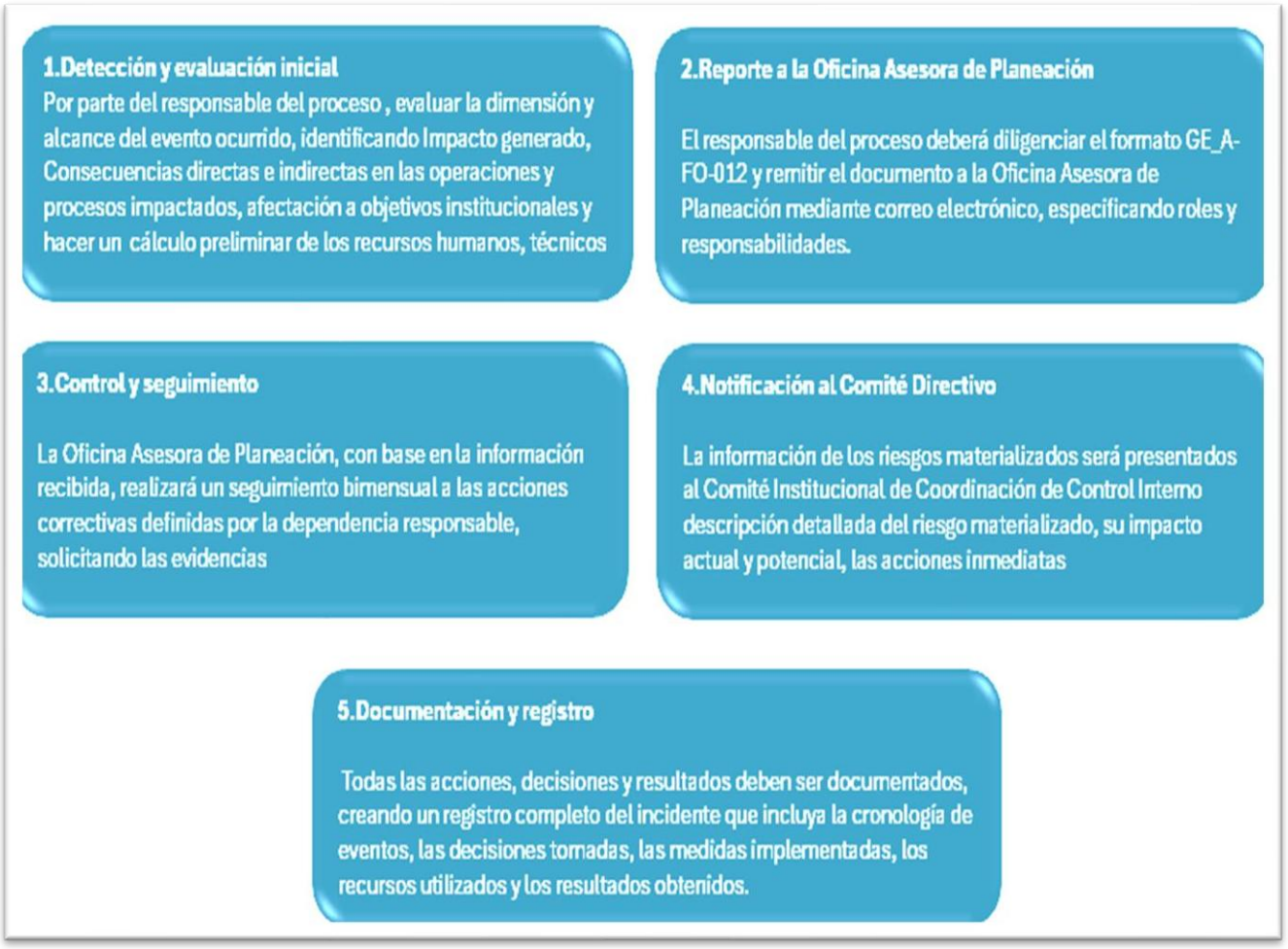


Ilustración 4 tratamiento de riesgos materializados
Fuente: Ministerio de Igualada y Equidad

10. ROLES Y RESPONSABILIDADES

El Ministerio de Igualdad y Equidad , estructura los criterios para la adecuada toma de decisiones respecto al tratamiento de los riesgos y sus efectos al interior de la entidad, por lo tanto, la implementación y mantenimiento de la Política de Administración de Riesgos, la metodología y tratamiento de los mismos, debe ser establecida por la Dirección con el apoyo del equipo directivo, el equipo operativo (líderes de proceso y gestores del Sistema de Gestión) y debe ser interiorizada por todos los servidores públicos y contratistas de la Entidad, responsables del desarrollo de actividades de los diferentes procesos.

Para la adecuada gestión de los riesgos de gestión, corrupción y de seguridad digital, el Ministerio de Igualdad y Equidad define los niveles de responsabilidad y autoridad acorde con las líneas de defensa definidas en la Entidad, con el fin implementar, coordinar, revisar, monitorear, hacer seguimiento y evaluar los riesgos inherentes a cada proceso.

Líneas de Defensa

Las Líneas de Defensa proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados. Este modelo proporciona una mirada a las operaciones, ayudando a asegurar el éxito continuo de las iniciativas de gestión del riesgo, y este modelo es apropiado para cualquier entidad – independientemente de su tamaño o complejidad" (IIA 2013:2). Las responsabilidades de la gestión de riesgos y del control están distribuidas en varias áreas y no se concentran en las oficinas de control interno; de allí que deban ser coordinadas cuidadosamente para asegurar que los controles operen. La adaptación este enfoque se presenta en la siguiente gráfica.

Líneas de defensa

LINEA ESTRATEGICA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
ALTA DIRECCIÓN Y COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO **Su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos**	Definir y aprobar la Política de Gestión de riesgos establecida en la presente política, para garantizar la implementación integral frente a riesgos de gestión, fiscales, de seguridad de la información, integridad publica y LA/FT/FPADM. Definir y aprobar la Política de Administración de Riesgos de la del Ministerio de Igualdad y Equidad, en el marco del Comité Institucional de Coordinación de Control Interno y el liderazgo del Representante Legal. Evaluar la Política de Administración de Riesgos, la cual debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, y dificultades para su desarrollo. Establecer los lineamientos y metodología para el tratamiento, manejo y seguimiento de los riesgos, incluyendo los riesgos de gestión, corrupción y de seguridad digital, que puedan afectar el logro de los objetivos institucionales. Establecer los roles y las responsabilidades frente a la Gestión de Riesgos de la Entidad incluyendo el responsable de Seguridad de la Información para la efectiva administración de los Riesgos de SD. Revisar y analizar los cambios en el "Direccionamiento estratégico", para la identificación de nuevos riesgos o la modificación de los que ya se tienen identificados, considerando los cambios en el entorno y los riesgos emergentes, que puedan afectar el cumplimiento de los objetivos estratégicos. Analizar los resultados del seguimiento de los riesgos estratégicos y de mayor impacto, para tomar acciones estratégicas que permitan mitigar la ocurrencia de los riesgos. Revisar en forma periódica el resultado del cumplimiento de los objetivos estratégicos y metas institucionales y de procesos, así como de los indicadores, para identificar posibles riesgos que se están materializando por no cumplimiento de estos.

Tabla 5 Roles y responsabilidades línea estratégica
Fuente: Manual Operativo MIPG V.4 DAFP- Guía Administración Riesgos V.6 DAFP

PRIMERA LÍNEA DE DEFENSA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
	Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro. establecimiento de actividades de control.
	Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos instituciones y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:
A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad. **Rol principal: diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la entidad.**	Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso. Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
	Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
	Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.

PRIMERA LÍNEA DE DEFENSA	
	Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos Informar oportunamente cualquier situación que pueda representar un conflicto de interés, amenazas contra la integridad publica como parte del deber ético y del compromiso con la transparencia institucional. Dichas situaciones deben ser comunicadas al responsable del proceso.

Tabla 6 Roles y responsabilidades primera línea de defensa
FUENTE: MANUAL OPERATIVO MIPG V.4 DAFP- GUÍA ADMINISTRACIÓN RIESGOS V.6 DAFP

SEGUNDA LÍNEA DE DEFENSA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
Conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia**)**.	Asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos.
Quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección	Hacer seguimiento a las actividades de manejo para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. Supervisores: alertar sobre la posible materialización de los riesgos identificados en la ejecución de los contratos
	Asesorar a la línea estratégica en el análisis del contexto interno y externo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
	Apoyar a la Alta Dirección en la estructuración y definición de la Política de Administración de riesgos Del Ministerio, para presentarla al Comité Institucional de coordinación de Control Interno- CICCI.
	Hacer seguimiento periódico a los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles.

SEGUNDA LÍNEA DE DEFENSA	
OFICINA DE PLANEACIÓN	Consolidar el Mapa de riesgos Institucional con los riesgos de corrupción y fraude y los riesgos de gestión calificados en zona moderada, alta y extrema.
	Realizar la difusión y asesoría de la metodología para la gestión de riesgos adoptada por El Ministerio
	Orientar y acompañar a los líderes de procesos en la gestión de riegos (gestión y corrupción) en cada una de sus etapas (Identificación, análisis, evaluación, establecimiento de controles y planes de manejo).
	Fomentar la administración del riesgo como una actividad inherente al proceso de Planeación Estratégica, trabajando en forma coordinada y armónica con la Oficina de Comunicaciones y el Grupo Interno de Control Interno.
	Revisar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisar que la implementación de los planes de manejo de los riesgos sea eficaz. Promover la implementación de los lineamientos institucionales para la prevención del riesgo de Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM), liderado por la Oficina asesora de Planeación en coordinación con Dirección Jurídica, Oficina de relacionamiento con la ciudadanía, como parte del enfoque integral de gestión del riesgo. Esta función incluye articular con el Programa de Transparencia y Ética Pública, fortalecer los controles en los procesos sensibles y realizar seguimiento a la debida diligencia en las relaciones contractuales de la Entidad.

Tabla 7 Roles y responsabilidades de la segunda línea de defensa
Fuente: Manual Operativo MIPG V.4 DAFP- Guía Administración Riesgos V.6 DAFP

TERCERA LÍNEA DE DEFENSA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO	Evaluar de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la 2ª línea de defensa.

	A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces se garantiza el cumplimento efectivo de los objetivos.
	Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. Asesorar proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos.
	Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.
	Comunicar a la Alta Dirección, sobre el resultado de la evaluación a la gestión de riesgos y los posibles cambios e impactos, en el cumplimiento de los objetivos institucionales. (riesgos de corrupción y posibles fraudes)
	Proporcionar información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.
	Le corresponde al GIT de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la Entidad, a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.
	Evaluar la eficacia de la gestión de riesgos en la Entidad, el diseño y efectividad de los controles e informar a la Dirección sobre la efectividad de estos. Intervenir en la gestión de los riesgos relacionados con el Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) a través del desarrollo de cuatro funciones: evaluar de manera independiente el sistema de administración del riesgo, apoyar su gestión, verificar los controles internos establecidos y efectuar seguimiento orientado a la mejora continua.

Tabla 8 operatividad de la tercera línea de defensa
Fuente: Manual Operativo MIPG V.4 DAFP- Guía Administración Riesgos V.6 DAFP

La periodicidad para el monitoreo o control y seguimiento a los riesgos y seguimiento de

los controles se establece en el numeral **23 y 25** del presente documento, de acuerdo con la calificación de los riesgos residuales.

Además de las líneas de defensa y las responsabilidades asignadas para la Administración de Riesgos, a continuación, se presentan las responsabilidades establecidas en el Modelo de Seguridad y Privacidad de la Información MSPI- dadas en la Estrategia de Gobierno Digital del MINTIC**,** al responsable de Seguridad Digital, quien debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica[1].

El responsable de Seguridad Digital será quien tenga las siguientes responsabilidades respecto a la Gestión de Riesgos de Seguridad de la Información (GRSDI):

ROLES Y RESPONSABILIDADES DE SEGURIDAD DIGITAL	
PRIMERA LÍNEA DE DEFENSA **Responsable de la seguridad de la Información**	Definir el procedimiento para la Identificación y Valoración de Activos.
	Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
	Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
	Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
SEGUNDA LÍNEA DE DEFENSA **Oficial de seguridad**	Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información
	Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).
	Definir el procedimiento o metodología para la Identificación y Valoración de Activos
	Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información.
	Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
	Supervisar la respuesta a incidentes, así como l investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
	Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres.
	Realizar y/o supervisar pruebas de vulnerabilidades sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información

tabla 9 Responsabilidades, riesgos, seguridad digital
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

11. DESCRIPCIÓN DEL RIESGO DE GESTIÓN, INTEGRIDAD PÚBLICA, SEGURIDAD DE LA INFORMACIÓN

Para la describir o redactar el riesgo en forma adecuada, de tal forma que permita una interpretación adecuada, se debe tener en cuenta:

Iniciar con la palabra **"POSIBILIDAD"** y seguidamente, analizar los siguientes aspectos:

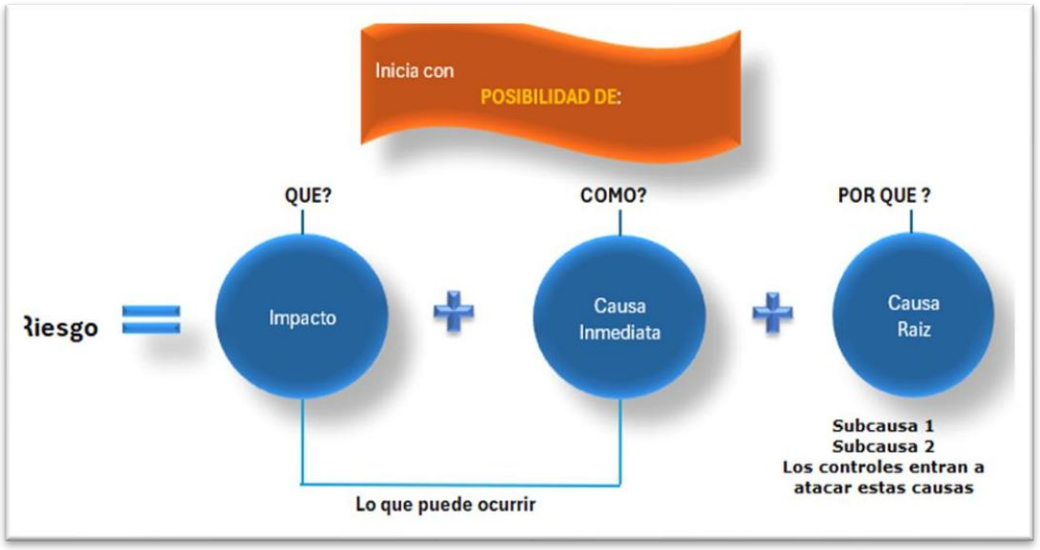


Ilustración 5 Descripción del riesgo
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

Es necesario identificar la causa inmediata (cómo) y la causa raíz (por qué), con el fin de que el riesgo quede bien identificado y su descripción evite interpretaciones subjetivas.

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

- **Causa inmediata**: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se

presente el riesgo.

Estos dos elementos permiten plantear el evento no deseado (¿Qué puede ocurrir?), es decir la situación, acción condición o suceso incierto que, si ocurre, podría afectar el logro de los objetivos de la entidad.

- **Causa raíz**: Se plantea ¿por qué puede ocurrir) el evento no deseado bajo el análisis de la causa principal o básica , corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo.

Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Premisas para tener en cuenta en la redacción del riesgo:

- **No** describir como riesgos omisiones ni desviaciones del control.
- **No** describir causas como riesgos
- **No** describir riesgos como la negación de un control.
- **No** existen riesgos transversales, lo que pueden existir son causas transversales

Para los riesgos de Seguridad de la información se identificará el riesgo con la probabilidad de perdida de confidencialidad, integridad o disponibilidad de la información, así como la amenaza (causa inmediata) y la vulnerabilidad (causa raíz)

La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en el numeral 12 de este documento. Todos iniciarán con la formula *"Posibilidad de"*, y deben señalar el impacto, la causa inmediata y la causa raíz.
Teniendo en cuenta las amenazas para la integridad pública, las causas inmediatas de los riesgos para la integridad pública podrán ser el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP.
De acuerdo con lo anterior, se sugiere tener en cuenta los siguientes ejemplos

Impacto	Causa inmediata	Causa raíz

Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]"	
	Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una	

Tabla 10 Ejemplos como referente para análisis del riesgo
Fuente: Guía para la gestión Integral del riesgo en Entidades Públicas V.7 2025

12. FACTORES DE RIESGO

Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

Factor	Definición	Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos definidos para la operación de la entidad, incluyendo el uso de sistemas de información y errores en actividades realizadas por los servidores. Incluye la estructura organizacional que afecta la capacidad institucional.	Falta de aplicación de procedimientos Falta de segregación de funciones Errores de grabación y autorización Falta de supervisión o interventoría
Transacción u Operación (aplica para LA/FT/FPADM)	Eventos relacionados con operaciones realizadas por un cliente o usuario, que implican entrega o recepción de recursos, bienes o servicios en una jurisdicción específica.	Errores en cálculos para pagos internos y externos Contrapartes (naturales o jurídicas) Productos (bienes o servicios) ofrecidos/requeridos Canales utilizados para la operación Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la integridad pública.	Alta rotación o insuficiencia de personal Acciones contrarias a normas laborales o de seguridad Acciones contrarias a acuerdos contractuales Falta de capacitación Fraude interno Soborno Gestión inadecuada de conflictos de interés Corrupción
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Hurto de activos tecnológicos Daño de equipos Caída de sistemas de información o aplicaciones Caída de redes Errores en hardware o software Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes Incendios Inundaciones Daños a activos fijos
Eventos externos	Eventos derivados de situaciones externas que afectan la entidad.	Fraude externo Suplantación de identidad Asaltos a la oficina Atentados, vandalismo y alteraciones de orden público

Tabla 11 Factores de riesgo
Fuente: Adaptado de la Guía de Gestión Integral del Riesgo V7 (DAFP)

12.1 Valoración de los Riesgos

La valoración de riesgos consiste en establecer la probabilidad de ocurrencia del riesgo y nivel de consecuencia del impacto, con el fin de estimar la zona de riesgo inicial-**RIESGO INHERENTE**[5].

Los elementos que se deben tener en cuenta para realizar la valoración son:

El análisis del riesgo: Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial o riesgo inherente.

Evaluación de riesgos: Se busca confrontar los resultados del análisis del riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final o riesgo residual.

12.2 Análisis de riesgos

La construcción de los riesgos se realiza a partir de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

12.3 Determinación de la probabilidad

La probabilidad o posibilidad de ocurrencia del riesgo, está asociada a la exposición del riesgo del proceso que se encuentra en análisis.

La probabilidad inherente: es el número de veces o frecuencia que se repite la actividad en un año.

La exposición al riesgo estará asociada al proceso o actividad que se esté analizando

12.4 Criterios para definir el nivel de probabilidad

Las tablas de calificación del impacto definidas para los Riesgos de Gestión, Integridad pública y Seguridad de la información se definen así:

PROBABILIDAD				
	Frecuencia de la Actividad	**Mínimo**	**Máximo**	**Probabilidad**
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	**0**	**2**	**20%**
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	**3**	**24**	**40%**
Moderado	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	**25**	**500**	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5.000 veces por año	**5001**	**5000**	**80%**
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año	**5001**		**100%**

Tabla 12 Criterios para definir el nivel de probabilidad
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

12.5 Determinación del Impacto.

Son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. Para establecer el impacto de los riesgos identificados, se toman las variables de IMPACTO ECONÓMICO y REPUTACIONAL, lo que permite que la evaluación del riesgo sea más objetiva.

En el caso de que se presenten ambas variables, se toma la que presente el mayor nivel más alto.

IMPACTO			
Nivel	**% Impacto**	**Afectación económica**	**Reputacional**
Leve	**20%**	Menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor	**40%**	Mayor a 10 y menor 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado	**60%**	Mayor a 50 y menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor	**80%**	Mayor a 100 y menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico	**100%**	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Tabla 13 Criterios para definir el nivel de impacto
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

El líder del proceso será quien determine los criterios de Probabilidad e impacta para el análisis del riesgo, que es quien conoce el proceso.

12.6 Análisis de severidad

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zona de severidad en la matriz de calor.

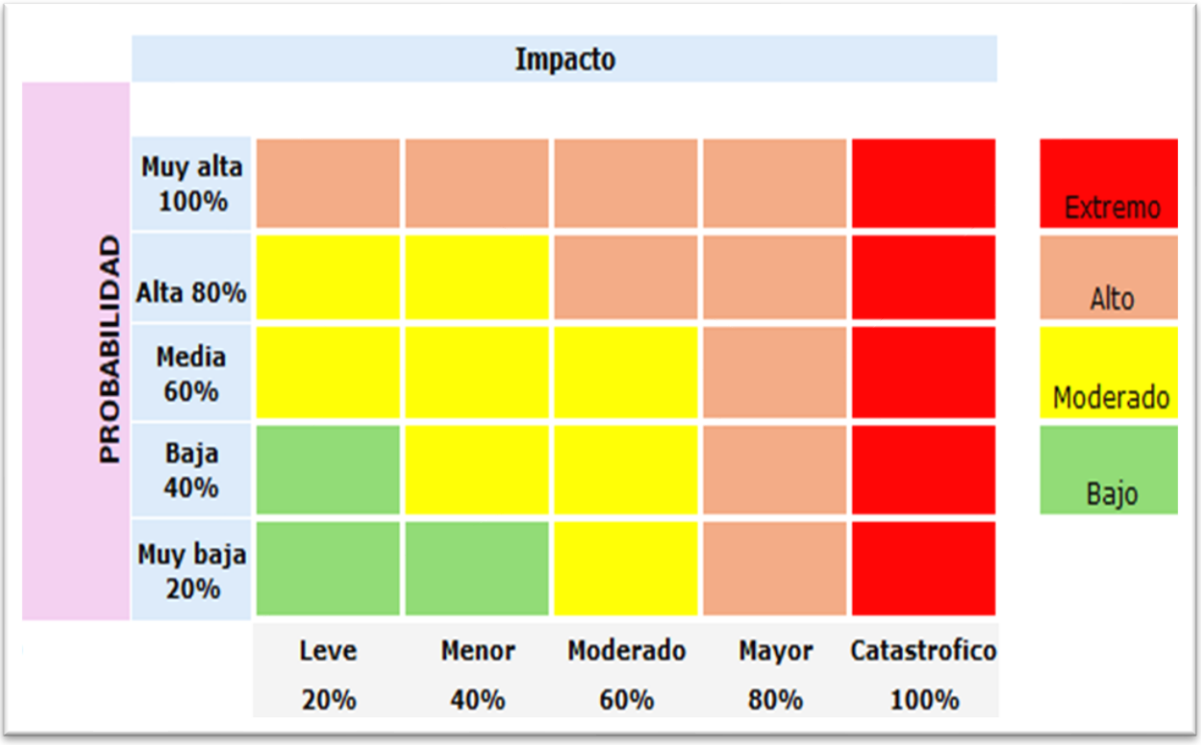


Tabla 14 Matriz de calor (niveles de severidad del riesgo)
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

12.7 Evaluación de los Riesgos

A partir del análisis de probabilidad e impacto, se establece la zona inicial que queda ubicado el riesgo inherente, en la tabla de calor.

Esta se determina mediante la combinación de la probabilidad y el impacto así:

%	MATRIZ CALIFICACIÓN DE RIESGOS IMPACTO					
100%	Muy alta	ALTA	ALTA	ALTA	ALTA	EXTREMA
80%	Alta	MODERADA	MODERADA	ALTA	ALTA	EXTREMA
60%	Media	MODERADA	MODERADA	MODERADO	ALTA	EXTREMA
40%	Baja	BAJA	MODERADA	MODERADO	ALTA	EXTREMA
20%	Muy baja	BAJA	BAJA	MODERADO	ALTA	EXTREMA

	PROBABILIDAD	LEVE	MENOR	MODERADO	MAYOR	CATASTROFICO
		20%	40%	60%	80%	100%
		IMPACTO				

tabla 15 Evaluación de riesgos
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

Como resultado de la evaluación los riesgos inherentes, se pueden ubicar en las siguientes zonas:

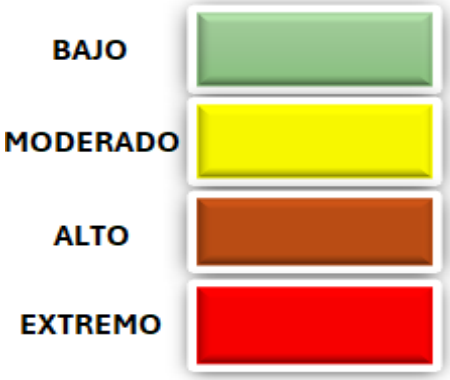


Tabla 16 Zonas de riesgo
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

Una vez se obtiene la calificación y zona donde queda ubicado el riesgo inherente, se continúa con el establecimiento de controles y la valoración de estos, permitiendo establecer el riesgo residual (después de controles).

13. DISEÑO Y ANÁLISIS DE CONTROLES

Las actividades de control son acciones concretas y con unos atributos específicos que son establecidas a través de políticas, procedimientos u otras directrices o documentos institucionales e implementadas con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos.

Estas se pueden diseñar y establecer para cada riesgo a través de diferentes mecanismos, bien sea a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos que el líder del proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo.

Se requiere considerar los diferentes atributos de las actividades de control para asegurar aspectos tales como: los responsables de su ejecución, la segregación de funciones y niveles de autoridad apropiados.

Las actividades de control deberán atender las causas raíz identificadas y enfocarse en la gestión de los factores de riesgo previamente identificados. Estas serán mayormente efectivas cuando cuenten con todos sus atributos y cuando estén directamente relacionadas con tales causas y factores de riesgo.

13.1 Estructura para la Descripción del Control:

Para un adecuado diseño de las actividades de control se propone una estructura para su redacción que agrupa los atributos necesarios para garantizar su implementación de forma efectiva por parte del responsable. La estructura propuesta se despliega en la siguiente ilustración.

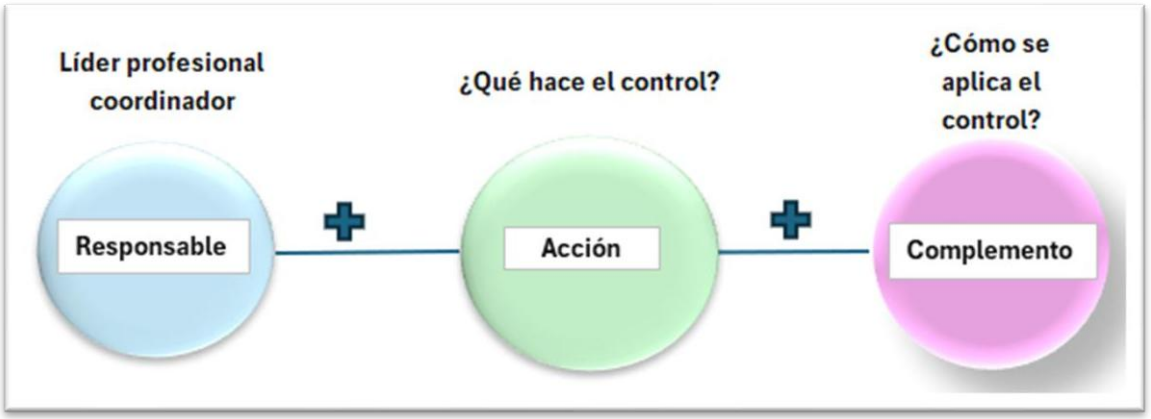


Ilustración 6 Estructura Redacción de controles
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7. 2025

La estructura básica de un control consta de los siguientes elementos:

1. **Responsable**. Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

2. **Periodicidad**. Debe tener una periodicidad (diario, mensual, trimestral, anual) etc. definida para su ejecución.

3. **Propósito**. Se determina mediante verbos que indican la acción (verificar, validar, conciliar, comparar, revisar, cotejar), que deben realizar como parte del control.

4. **¿Cómo se realiza el control?** Corresponde a los detalles que permiten identificar claramente el objeto del control.

5. **Observaciones y desviaciones**. Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.

6. **Evidencia** de la ejecución del control.

13.2 Tipologías de Controles

Con el fin de establecer la tipología de controles para su posterior validación, es necesario acudir al cicl9.3o de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo, o bien una combinación de estos.

Controles Preventivos: Son los que actúan en la entrada del proceso y antes de que

se realice la actividad que origina el riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Controles Detectivos: Son los que actúan durante la ejecución de la actividad. Detectan el riesgo, pero generan reproceso.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen pueden generar costos implícitos.

De acuerdo con la forma como se ejecutan los controles, se clasifican en:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

Las actividades de control tienen como fin:

TIPO DE CONTROL	RESULTADO	ETAPAS DEL PROCESO
Controles Preventivos	Va a las causas del riesgo Atacan la probabilidad de ocurrencia del riesgo	Entradas
Controles Detectivos	Detecta que algo ocurre y devuelve el proceso a los controles preventivos Atacan la probabilidad de ocurrencia del riesgo	Ejecución de actividades
Controles Correctivos	Atacan el impacto frente a la Materialización del riesgo	Salidas

Tabla 17 Actividades de control
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

13.3 Valoración de los Controles:

Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó.

Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

13.4 Resultados de la evaluación del diseño del control

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la

calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

R A N G O D E CALIFICACIÓN DEL DISEÑO	RESULTADO PESO DE LA EVALUACION DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Tabla 18 Resultados de la evaluación del diseño del control

El control debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. Debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoria interna o control interno.

Rango de calificación de la ejecución	Resultado Peso de la ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Tabla 19 Rango de calificación y peso del control

13.5 Atributos para el diseño de los controles.

Para el diseño de los controles, se tienen en cuenta dos clases de atributos: Atributos de eficiencia y Atributos informativos.

Los atributos de eficiencia dan una evaluación al control cuantitativa, lo cual permite determinar la efectividad del control y establecer la evaluación final del riesgo, al

moverse en la matriz de calor (riesgo residual), de acuerdo con el tipo de control y disminuir la probabilidad o el impacto.

Los atributos informativos, sólo dan formalidad al control, permitiendo conocer el entorno del control de forma cualitativa, estos no generan calificación en la evaluación del control.

Tabla 21 Atributos para los controles
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

CARACTERISTICAS			DESCRIPCIÓN	PESO
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se puede generar reprocesos	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automaticas en la intervencion de personas para su realización	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano	15%
VALORACIÓN DEL CONTROL 90%				
Atributos Informativos	Documentación	Documentado	Controles que estan documentados en el proceso ya sea manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	´-
		Sin documentar	identifica a los controles que pese a que se ejecutan en el proceso no se encuentan documentados en ningun documento propio del proceso	´-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva al riesgo	´-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva al riesgo.	´-
	Evidencia	Con registro	El control deja un registro, permite evidencia de la ejecución del control.	´-
		Sin registro	El control no deja registro, de la ejecución del control.	´-

13.6 Aplicación de los Controles en la matriz de severidad:

Teniendo en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor, a continuación, se muestran cual es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

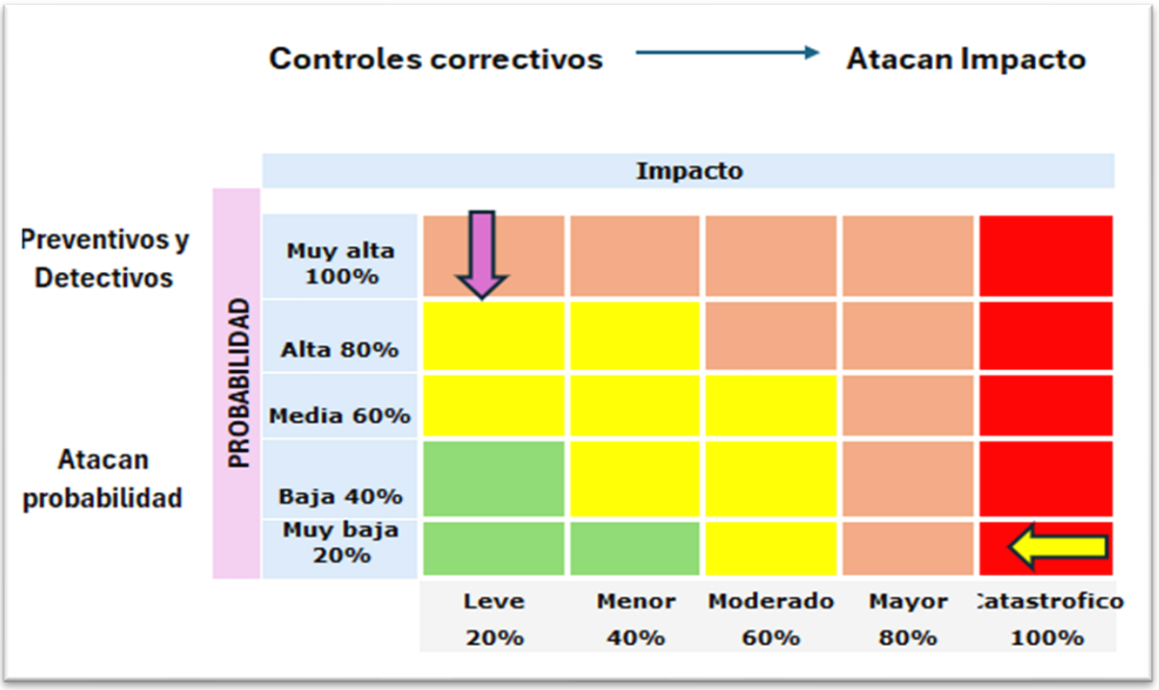


Tabla 20 Movimiento en la matriz de calor acorde con el tipo de control
Fuente: Adaptada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7-2025

14. VALORACIÓN DEL RIESGO

Riesgo Residual

Desplazamiento del riesgo inherente para calcular el riesgo residual

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES.	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
moderado	Directamente	Directamente	1	1
moderado	Directamente	Indirectamente	1	0
moderado	Directamente	No disminuye	1	0
moderado	No disminuye	Directamente	0	1

Tabla 21 Nivel del riesgo

Fuente: Adaptada de la Guía para la Gestión Integral del Riesgo en Entidades Públicas

IMPORTANTE Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

IMPORTANTE Tratándose de riesgos de corrupción únicamente hay disminución de Probabilidad. Es decir para el impacto no opera el desplazamiento.

Para la aplicación de los controles se debe tener en cuenta que los controles mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control[7].

Ejemplo de aplicación.

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Calculos requeridos
	Valoración de probabilidad				
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%*40%=24% 60%-24%=36%
	Valoración probabilidad para aplicar 2 do control				36%
	Valoración control 2 detectado			30%	36%*30%=10,8% 36%-10%=25,2%
	Probabilidad Residual				25,20%
	Valoración del Impacto				
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual				80%

Tabla 22 aplicación de controles para establecer el riesgo residual
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

Movimiento en la matriz de calor del ejemplo.

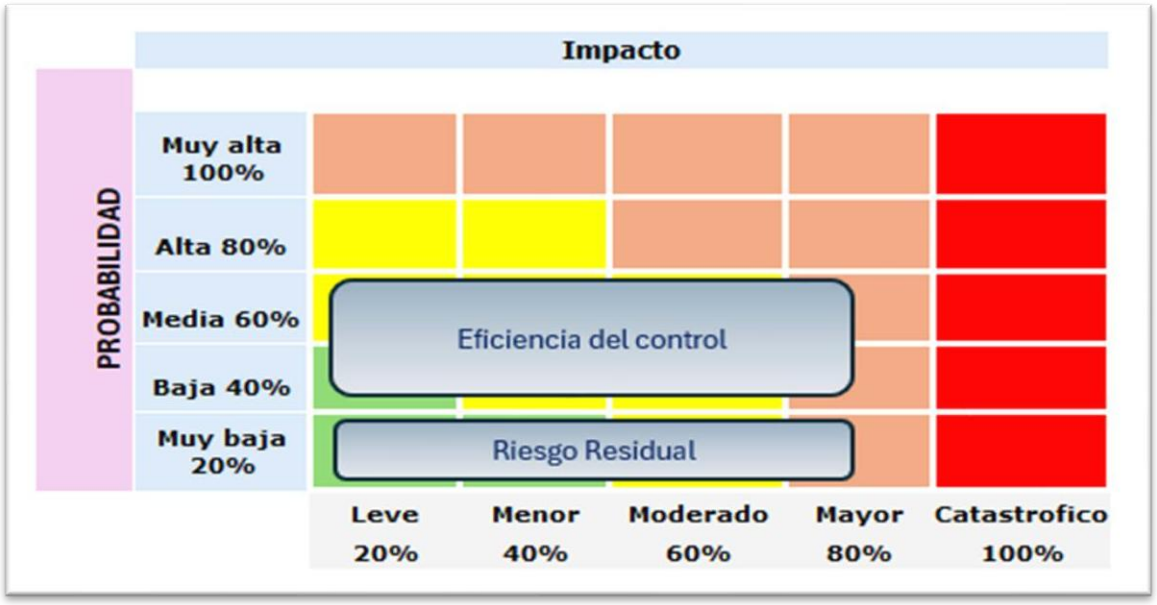


Tabla 23 Movimiento de la matriz de calor del ejemplo
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

Para la identificación, valoración de controles se cuenta con la Matriz Mapa de Riesgo GE-A-FO-006 y la de seguridad de la información TI_S-FO-003**,** la cual se adoptó del formato del DAFP, anexo de la Guía de Administración de Riesgos y establecimiento de controles V.7-2025.

Consolidación Mapa de Riesgos Integral:

A partir de la aplicación de cada uno de los pasos metodológicos se procede con la elaboración y consolidación del mapa integral de riesgos.

Este formato se encuentra parametrizado y el cual genera la calificación del riesgo residual de conformidad con la clase de control, evaluación de sus atributos y generación del resultado final de acuerdo con la evaluación final de los controles que se identifiquen para cada riesgo.

EVALUACIÓN DEL RIESGO - VALORACIÓN DE LOS CONTROLES									EVALUACIÓN DEL RIESGO- NIVEL DEL RIESGO RESIDUAL					
			ATRIBUTOS											
No de control	Descripción del control	Afectación	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual final	%	Impacto Residual final	%	Zona Residual Final	Tratamiento
1		Probabilidad	Detectivo	Manual	30%	Sin documentar	Continua	Con registro	Baja	28%	Leve	20%	Bajo	Aceptar

Tabla 24 Evaluación del riesgo
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

14.1 Tratamiento de riesgos residuales

El tratamiento o manejo de riesgos, es el conjunto de medidas que se toman, con el fin de tratar los riesgos y mitigar su materialización a través de la toma de medidas o acciones para su mitigación.

RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL			
CALIFICACIÓN	**POLITICA MANEJO DEL RIESGO**	**PLAN DE MANEJO**	**PLAN DE CONTINGENCIA**
Zona baja	**Asumir o aceptar el riesgo**	Riesgos inherentes, no se adoptan medidas que afecten la probabilidad o el impacto. Realizar monitoreos periódicos, semestral o trimestralmente, realizar controles para que permanezcan en zona baja.	**NA**
Zona Moderado	**Reducir el riesgo**	Establecer acciones, medidas que permitan reducir la probabilidad y/o el impacto del riesgo. Monitoreos periódicos, mínimo cada trimestre	**NA**
Zona Alta	**Evitar el riesgo**	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad y/o el impacto. Monitoreo bimensual a los controles y acciones establecidas.	Es optativo establecer planes de contingencia, para aplicar en caso de que el riesgo se materialice.

Zona Extrema	**Evitar el riesgo Compartir o transferir el riesgo**	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando tanto la probabilidad y/o impacto. Monitoreo mensual a los controles y acciones establecidas.	Establecer planes de contingencia para aplicar en caso de que el riesgo se materialice.

Tabla 25 Riesgos de gestión y de seguridad digital
Fuente: Anexo 4 MINTIC

Con base en el **formato GE-A—FO-006** Mapa de Riesgos, cada líder de proceso y el gestor(es), junto con su equipo de trabajo, de acuerdo con la calificación y la zona de riesgo que haya quedado ubicado el riesgo, establecen el tratamiento para cada uno, de conformidad con las Políticas de Administración adoptadas por el Ministerio.

RIESGOS DE CORRUPCIÓN			
CALIFICACION	**POLITICA MANEJO DEL RIESGO**	**PLAN DE MANEJO**	**PLAN DE CONTINGENCIA**
Zona baja	**REDUCIR EL RIESGO**	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad de ocurrencia. Monitoreos periódicos, mínimo cada trimestre a los controles y acciones.	
Zona Moderado			
Zona Alta	**EVITAR EL RIESGO**	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando la probabilidad de ocurrencia. Monitoreos bimensuales o mensuales a los controles y acciones establecidas	Establecer planes de contingencia para aplicar en caso de materialización
Zona Extrema			

Tabla 26 tratamiento de riesgos de corrupción
Fuente: Ministerio de Igualada y Equidad

Consolidación Mapa de Riesgos Integral:

A partir de la aplicación de cada uno de los pasos metodológicos se procede con la elaboración y consolidación del mapa integral de riesgos, para tal efecto se diligencia

una matriz descriptiva, acompañada de un esquema grafico que resume los análisis adelantados y permite contar con una visión integral de las diferentes tipologías de riesgos aplicables a cada proceso.

14.2 Análisis de riesgos de Integridad Publica

La gestión de los riesgos de integridad pública constituye un eje transversal y prioritario dentro del proceso de Administración del Riesgos. Estos riesgos hacen referencia a situaciones que pueden comprometer la legalidad, transparencia, imparcialidad y confianza en la gestión pública, y cuya materialización afecta seriamente la credibilidad institucional, el patrimonio público y el cumplimiento de los principios del buen gobierno.

De acuerdo con los lineamientos del Departamento Administrativo de la Función Pública (DAFP), el Programa de Transparencia y Ética Pública, los riesgos de integridad pública deben analizarse de manera diferenciada según su tipología. Estas incluyen: corrupción, conflicto de interés, fraude, soborno y riesgos asociados al Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM). Cada una representa mecanismos específicos de desvío de poder público para beneficio privado o para facilitar actividades ilícitas a través de la estructura institucional.

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado

Una vez se haya realizado el ejercicio de la identificación de riesgos de Integridad publica en el formato GE-A-FO-006 Mapa de Riesgos, se registran los riesgos identificados, correspondiente a cada proceso, se clasifican de acuerdo con tipo de riesgo que pertenezca; en este caso fraude interno o fraude externo.

14.3 Valoración de los riesgos de Integridad Pública

14.3.1 Cálculo de la probabilidad e impacto

Análisis de la probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda

NIVEL		DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de 1 vez al año
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	**Posible**	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
2	**Improbable**	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o normales)	No se ha presentado en los últimos 5 años

Tabla 27 Valoración de los riesgos de corrupción
Fuente: Adoptado - Adaptada de Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

14.3.2 Criterios para calificar la probabilidad

Para la valoración de los riesgos de corrupción, se determina la probabilidad de acuerdo con la metodología establecida para los riesgos de gestión, descrita en el presente manual y se clasifican, según la tabla de frecuencia y probabilidad.

PROBABILIDAD				
	Frecuencia de la Actividad	**Mínimo**	**Máximo**	**Probabilidad**
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	**0**	**2**	**20%**
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	**3**	**24**	**40%**
Moderado	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	**25**	**500**	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5.000 veces por año	**5001**	**5000**	**80%**

Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año	**5001**		**100%**

Tabla 28 Criterios para definir el nivel de probabilidad
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

Para el cálculo de la probabilidad, se hace necesario resaltar que la frecuencia a la que se hace referencia para los riesgos de corrupción se relaciona con la ejecución de la actividad de la cual proviene el riesgo de corrupción. Es decir, se debe considerar desde el objetivo del proceso y su exposición al riesgo[9].

14.3.3 Determinación del impacto.

Para determinar el impacto de los riesgos de corrupción, se tiene en cuenta los siguientes criterios, de acuerdo con el cuadro CRITERIOS PARA CALIFICAR EL IMPACTO -RIESGOS DE CORRUPCIÓN, el cual permite establecer la zona de impacto de los riesgos de corrupción de acuerdo con las siguientes preguntas:

CRITERIOS PARA CALIFICAR EL IMPACTO -RIESGOS DE CORRUPCION		
PREGUNTA: SI EL RIESGO SE MATERIALIZA PODRÍA:	**SI**	**NO**
1 ¿Afectar al grupo de funcionarios del proceso?		
2 ¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3 ¿Afectar el cumplimiento de misión de la		
3 ¿Afectar el cumplimiento de misión de la entidad?		
4 ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5 ¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6 ¿Generar pérdida de recursos económicos?		
7 ¿Afectar la generación de los productos o la prestación de servicios?		
8 ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9 ¿Generar pérdida de información de la entidad?		
10 ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11 ¿Dar lugar a procesos sancionatorios?		
12 ¿Dar lugar a procesos disciplinarios?		
13 ¿Dar lugar a procesos fiscales?		
14 ¿Dar lugar a procesos penales?		
15 ¿Generar pérdida de credibilidad del sector?		
16 ¿Ocasionar lesiones físicas o pérdida de vidas humanas	**CATASTROFICO**	
17¿Afectar la imagen regional?		

18 ¿Afectar la imagen nacional?		
19 ¿Generar daño ambiental?		
SUMA DE X's	0	0

Tabla 29 Criterios para calificar el impacto de riesgos de corrupción
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

CALIFICACIÓN IMPACTO	
RESPUESTAS POSITIVAS	**IMPACTO**
1 A 5	**MODERADO**
6 A 11	**MAYOR**
12 A 19	**CATASTRÓFICO**
Si la pregunta 16 es afirmativa es Catastrófico	

Tabla 30 Calificación de impacto
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

14.3.4 Determinación del riesgo inherente y residual.

Para la determinación del riesgo inherente (antes de controles) y residual, se realiza de acuerdo con lo establecido para los riesgos de gestión, a través de la matriz de calor para establecer la calificación inicial del riesgo.

%	MATRIZ CALIFICACIÓN DE RIESGOS IMPACTO						
100%	Muy alta	ALTA	ALTA	ALTA	ALTA	EXTREMA	
80%	Alta	MODERADA	MODERADA	ALTA	ALTA	EXTREMA	
60%	Media	MODERADA	MODERADA	MODERADO	ALTA	EXTREMA	
40%	Baja	BAJA	MODERADA	MODERADO	ALTA	EXTREMA	
20%	Muy baja	BAJA	BAJA	MODERADO	ALTA	EXTREMA	
	PROBABILIDAD	LEVE 20%	MENOR 40%	MODERADO 60%	MAYOR 80%	CATASTROFICO 100%	
		IMPACTO					

Zona de calificación riesgos de

Tabla 31 Matriz de evaluación del riesgo de corrupción
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

14.3.5 Control y seguimiento

El tratamiento de los riesgos de integridad pública debe realizarse de forma diferenciada según la tipología identificada, considerando su naturaleza, causas frecuentes, actores involucrados y canales de control institucional disponibles. En todos los casos, el enfoque debe ser de tolerancia cero, sin aceptación del riesgo residual, priorizando acciones de prevención, detección temprana y eliminación de condiciones de riesgo.
El control y seguimiento será el establecido en el numeral **11.1** del presente documento. Adicionalmente deberá contar con la asignación de la función de cumplimiento quien estará encargado de velar por el efectivo, eficiente y oportuno funcionamiento del SIGRIP en su conjunto, y cada uno de sus elementos, promoviendo el cumplimiento de sus disposiciones y apoyando a los líderes de procesos y gestores de riesgo, en la gestión de los riesgos identificados.

15. ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El análisis de riesgos de seguridad de la información es un instrumento desarrollado por el Ministerio de las Tecnologías de la Información y de las Comunicaciones que imparte los lineamientos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información basado en las normas y estándares de mejores prácticas en materia de seguridad de la información.

15.1 Identificación de activos de seguridad de la Información

para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas"

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento. Es necesario que la entidad pública identifique los activos y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano

(FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado. La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública. Para la generación de este inventario, la entidad pública debe tener en cuenta los siguientes pasos.

Tabla 32 Identificación de los activos de información

Fuente: Pasos para la identificación y valoración de activos. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Para cada activo se define el nivel de criticidad de la propiedad específica, para cada propiedad "se definieron tres (3) niveles que permiten determinar el valor general o criticidad del activo en la entidad": Alta, Media y Baja, que corresponden con Criterios de Clasificación para cada una de las propiedades de la Información.

15.2 Matriz de Riesgos de Seguridad de la Información:

Con base en la criticidad se realiza el proceso de gestión de riesgos, la cual registra en la Matriz de Riesgos de Seguridad de la Información, con respecto al activo de información se registran los siguientes datos:

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN			
Proceso	Referencia	Activo de información	Tipo de Activo

Tabla 33 Matriz de riesgos de seguridad de la información
Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

15.3 Identificación de áreas de impacto

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

15.4 Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).
Pueden ser Deliberadas (D), fortuitas (F) o ambientales (A)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

15.5 Descripción del riesgo

A partir del punto de riesgo, área de impacto y área(s) de factor(es) de riesgo identificados, se debe proceder con la descripción del riesgo.
La estructura es la definida en el numeral 12 de este documento

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

Tabla 34 Riesgos de seguridad de la información
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

15.6 Clasificación del Riesgo:

Este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad.
A partir de este paso metodológico se incorporan la tablas y matrices establecidas en el numeral 12.2 valoración del riesgo inherente, nivel de probabilidad numeral 12.2.,12.2.3 tabla 13, determinación del impacto numeral 12.2.4 tabla 14 y análisis de severidad

numeral 12.2.5 tabla 15 del presente documento.

ID ACTIVO	NOMBRE DEL ACTIVO	NIVEL DE CRITICIDAD ACTIVO	ICC			
			SOCIAL 250.000 PERSONAS	ECONOMICO	AMBIENTAL	SE DEBE REPORTAR A CCCI
		Indicar Nivel de	Indicar con	Indicar con una X si hay afectación económica	Indicar con	Indicar con
Indicador	Indicador	criticidad,	una X si		una X si	una X si se
ID del	nombre del	definido en la	hay		Hay	debe
activo	activo	tabla de registro	afectación		afectación	reportar a
		de activos	social		ambiental	CCOCI

Tabla 35 Indicadores de infraestructura
Fuente: Modelo de gestión de riesgos de seguridad digital MINTIC

15.7 Metodología para la identificación de riesgos de Seguridad de la información.

El propósito de la identificación de los riesgos de Seguridad de la información, es determinar que podría suceder para que cause una perdida potencial, y llegar a comprender el cómo, el dónde, y el por qué podría ocurrir está perdida. Las siguientes etapas del análisis de riesgos de SD se requieren para recolectar datos de entrada para esta actividad.

Para la identificación de los riesgos inherentes El Ministerio de Igualdad y Equidad tiene en cuenta las amenazas y vulnerabilidades asociadas a cada activo de información.

Se identifican tres (3) clases de riesgos inherentes a seguridad digital:

Integridad: se refiere a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros no autorizados.

Confidencialidad: se refiere a cómo los datos se mantienen al acceso únicamente de las personas o sistemas que se encuentran autorizados.

Disponibilidad: se refiere al acceso de la información en el momento que debe estar disponible; se aclara que la información de la entidad no debe estar disponible todo el

tiempo durante el año

"La gestión de riesgos en seguridad de la información que cubre la identificación, valoración y evaluación de riesgos se realiza tomando como insumo la identificación de los activos de información, posterior a ello, se realizan mesas de trabajo con el responsable de seguridad de información y cada uno de los líderes de proceso (o a quien este designe). La valoración de los riesgos se hace a través
de juicios de experto y cuando aplique, basado en datos previos con los que cuente la Entidad. Finalmente, una vez identificado los riesgos de seguridad, y de acuerdo con los niveles de valoración y aceptación, se define en conjunto con el líder de proceso la propuesta de plan de tratamiento de riesgos para ser revisado, aprobado, implementado y monitoreado por las partes."

NOTA: *Para efectos de gestión de riesgos se considerarán aspectos de la metodología de gestión de riesgos establecida por el Departamento de la Función Pública, de la cual se extraerán elementos que se consideren pertinentes, sin obligatorio cumplimiento en su totalidad.*
En el siguiente numeral, se detallan algunas amenazas que pueden hacer daños a los activos y materializar los riesgos y algunas vulnerabilidades (debilidades) descritas en el *anexo 4. Lineamientos para la GRSD y complementadas por la Guía De Gestión De Riesgos emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Digital para la Seguridad y privacidad de la información.*

De acuerdo con lo descrito en la *Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas" del DAFP,* para la identificación del riesgo y el análisis de las posibles amenazas y vulnerabilidades que podrían causar la materialización de este, El Ministerio de Igualdad y Equidad ha adoptado la siguiente tabla:

Riesgo	Descripción del riesgo	Activo	Tipo de Activo	Amenaza	Vulnerabilidades	Consecuencia / Impacto
Identificar el tipo de riesgo de acuerdo con la identificación n establecida	Detallar el riesgo	Asociar activo o grupo de activos según lo identificad o en el formato de registro de activos de información	Detallar el tipo de Activo de información	Detallar la amenaza a la cual stá expuesta el grupo de activo	Describir cuales son las vulnerabilidades asociadas a la amenaza Identificada.	Describir las consecuencias que tendría el grupo de activos al verse afectado por la amenaza asociada.

Tabla 36 Guía para la administración del riesgo
Fuente: Guía para la administración del riesgo DAFP v6

15.8 Establecimiento de controles de riesgos de Seguridad de la información

Para establecer los controles para los riesgos de Seguridad de la información se debe tener en cuenta:

Los tipos de controles aplicables a los riesgos de seguridad de la información son los mismos establecidos para los riesgos de gestión, cuya definición, clasificación y valoración se encuentran detallados en el numeral 13 del presente documento.

El Modelo de Seguridad y Privacidad de la Información del Ministerio de Igualdad y Equidad en su fase de Planificación deberá realizar la selección de controles de seguridad de la información que correspondan para el tratamiento del riesgo, y durante la fase Implementación deberá ejecutar la implementación de dichos controles, por lo cual se cuenta con el anexo de controles del estándar ISO 27001.

NOTA: *El Ministerio deberá determinar si ya posee alguno de estos controles del Anexo A de la Norma ISO 27001 2022 o si deberá aplicar alguno para realizar luego el tratamiento del riesgo residual.*

15.9 Identificación y evaluación de controles Seguridad de la Información

Para los casos en los cuales se determine Reducir el Riesgo o Compartir el riesgo se deben estructurar controles que cumplan con las características establecidas en el presente documento.

Tipo de controles

Los tipos de controles son los mismos que se han establecido para los riesgos de gestión corrupción, estos son:

Controles Preventivos: Son los que actúan en la entrada del proceso y antes de que se realice la actividad que origina el riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Controles detectivos: Son los que actúan durante la ejecución de la actividad. Detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen pueden generar costos implícitos.
De acuerdo con la forma como se ejecutan los controles, se clasifican en:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

Se propenderá estructurar un Control que permita dar cobertura de carácter preventivo, detectivo y correctivo, los cuales deben tener las características de un control.

Los controles de Seguridad de la información tienen las mismas características de los riesgos de gestión y corrupción, conforme a la metodología establecida del presente documento.

16. ANÁLISIS DE RIESGO FISCAL

Para el establecimiento de los riesgos de corte fiscal, El ministerio toma como base, la metodología establecida en la **Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7.**

El riesgo fiscal es: "Es el efecto dañoso sobre los recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial"[10].

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

Efecto dañoso: es el daño que se generaría sobre los recursos los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal= Evento Potencial (Potencial conducta) + Efecto dañoso (Potencial daño)

No se debe confundir el riesgo fiscal con el daño patrimonial El riesgo fiscal se relaciona con el evento de potencial efecto perjudicial sobre los recursos, bienes o intereses públicos, mientras que el daño patrimonial es la afectación real y concreta a los mismos, como resultado de una acción u omisión.

16.1. Identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario tener en cuenta los siguientes pasos

Ilustración 7 Pasos para la identificación del riesgo fiscal

Fuente: Adoptado de la Guía para Gestión Integral del Riesgo en Entidades Públicas Versión 7 2025

16.1.1. Puntos de riesgo y circunstancias inmediatas

Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica -causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Por cada punto de riesgo, con frecuencia existen múltiples circunstancias inmediatas. La identificación de los puntos de riesgo y las circunstancias inmediatas han de ser el resultado del trabajo conjunto entre el personal directivo, asesor y demás servidores que por su experiencia o formación puedan aportar al análisis crítico y objetivo de la gestión fiscal de la entidad. Para este ejercicio, se sugieren las siguientes preguntas orientadoras:

Preguntas y criterios para la identificación	Sirve para identificar
¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal)	Puntos de riesgo fiscal

¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo 1), son aplicables a la entidad?	Puntos de riesgo fiscal y circunstancias inmediatas
Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces. En un ejercicio autocrítico, realista y objetivo, ¿cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.	Puntos de riesgo fiscal y circunstancias inmediatas

Tabla 37 Preguntas orientadoras para identificar puntos de riesgo fiscal y circunstancias inmediata

16.1.2. Identificación de áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la

organización en caso de materializarse el riesgo.

Para definir de manera correcta el área de impacto, al momento de identificar y redactar riesgos fiscales, es fundamental tener claro el concepto de patrimonio público a partir de las tres expresiones que se derivan del artículo 6 de la Ley 610 de 2000:

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Son todos aquellos muebles e inmuebles de propiedad pública (bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público (aquellos cuyo uso pertenece a todos los habitantes del territorio nacional) y bienes fiscales (aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos).	Son los dineros comprometidos y ejecutados en ejercicio de la función pública.	Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica.

Tabla 38 Bienes Públicos
Fuente: Adoptado de la Guía para Gestión Integral del Riesgo en Entidades Públicas Versión 7 2025

16.1.3. Identificar el efecto económico

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

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

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

- Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.

- Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de

gestor público

16.1.4. Identificación de la causa raíz o potencial hecho generador

Corresponde al por qué; que es el evento (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

Al ser la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador. Es fundamental entonces, deslindar el hecho que ocasiona el daño (evento potencial o causa raíz), del daño propiamente dicho.

16.2 Descripción del Riesgo Fiscal

Para redactar un riesgo fiscal se debe tener en cuenta:

Iniciar con la oración: *Posibilidad de,* debido a que nos estamos refiriendo al evento potencial.

Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica - causa raíz- para que se presente el riesgo.

Causa Raíz: corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño. Es la condición necesaria del riesgo, de tal forma que, si ese hecho no se produce, el daño no se genera.

Ilustración 8 Descripción riesgo Fiscal

Fuente: Adoptado de la Guía para Gestión Integral del Riesgo en Entidades Públicas Versión 7 2025

16.3 Valoración del Riesgo Fiscal

Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

16.3.1 Determinación de la probabilidad

Para la valoración de los riesgos fiscales, se determina la probabilidad de acuerdo con la metodología establecida para los riesgos de gestión y se clasifican, según la tabla de frecuencia y probabilidad.

PROBABILIDAD				
	Frecuencia de la Actividad	**Mínimo**	**Máximo**	**Probabilidad**
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	**0**	**2**	**20%**
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	**3**	**24**	**40%**
Moderado	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	**25**	**500**	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5.000 veces por año	**5001**	**5000**	**80%**
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año	**5001**		**100%**

Tabla 39 Criterios para definir el nivel de probabilidad
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

16.3.2 Determinación del Impacto

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso recae sobre un bien, recurso o interés patrimonial de naturaleza pública. Toda potencial consecuencia económica sobre el patrimonio público, es relevante, sin embargo, existen niveles para su valoración**.**

IMPACTO			
Nivel	**% Impacto**	**Afectación Económica**	**Reputacional**
Leve	**20%**	Menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor	**40%**	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado	**60%**	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor	**80%**	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico	**100%**	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Tabla 40 Evaluación de los riesgos
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2025 V.7

16.3.3 Determinación del riesgo inherente y residual

Para la determinación del riesgo inherente (antes de controles) y residual, se realiza de acuerdo con lo establecido para los riesgos de gestión, a través de la matriz de calor para establecer la calificación inicial del riesgo. Ver Numerales 9.4 del presente documento.

16.4 Valoración de Controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Los controles pueden ser preventivos, detectivos o correctivos dependiendo el momento

(antes, durante o después) en que se accionen respecto a la actividad que origina el riesgo fiscal (punto de riesgo). Los controles preventivos buscan asegurar que no se presente la causa raíz, los controles detectivos buscar tomar medidas ante la ocurrencia de la causa raíz para evitar que se produzca el efecto dañoso y los controles correctivos actúan ante el daño potencial, procurando detener su materialización o reparando el daño causado.

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Se aplican los lineamientos para la redacción del control establecidos en los numerales 9.6 de la presente guía.

17. MAPAS DE RIESGOS

El mapa de riesgo es el consolidado de los riesgos identificados en cada proceso, los riesgos residuales, planes de manejo y planes de contingencia. El mapa de cada proceso cuenta con el Formato GE-A-FO-006 Mapa de Riesgos**.**
Los mapas de riesgos permiten llevar el control de los riesgos, a nivel de proceso y a nivel estratégico.

Los Mapas de Riesgo son consolidados por la Oficina de Planeación y se clasifican en:

Mapa de Riesgo de Proceso: El cual contiene los riesgos identificados en cada uno de los procesos. Estos mapas deben ser revisados por el director, subdirector, jefe de Oficina, Coordinador de Grupo o Líder de Proceso; y deben ser aprobados por el Líder del Proceso.

Mapa de Riesgo de Institucional: El cual consolida los riesgos identificados en cada proceso calificados en zona alta y extrema y los riesgos de corrupción. Este es consolidado por la Oficina de Planeación.

18. MONITOREO Y SEGUIMIENTO

18.1 Monitoreo de los riesgos y controles

El monitoreo a los mapas de riesgos es esencial para asegurar la eficiencia y eficacia de las acciones establecidas para el tratamiento de los riesgos de gestión, seguridad de la información, fiscal y de Integridad Publica

18.1.1 Indicadores Clave de Riesgo (KRI)

Los Indicadores Clave de Riesgo corresponden a métricas de monitoreo utilizadas para identificar variaciones, tendencias, acumulaciones, desviaciones o comportamientos que puedan evidenciar incremento en la exposición al riesgo, debilitamiento de controles o posibles condiciones asociadas a la materialización de eventos de riesgo en los procesos institucionales.

Constituyen mecanismos de seguimiento preventivo orientados a fortalecer la gestión anticipada de los riesgos y apoyar la toma de decisiones oportunas por parte de las líneas de defensa.

Los Indicadores Clave de Riesgo (KRI) tendrán como finalidad fortalecer el monitoreo continuo de los riesgos institucionales mediante la generación de alertas tempranas que permitan:

- Identificar oportunamente cambios en los niveles de exposición al riesgo.
- Detectar posibles desviaciones en la efectividad de controles y actividades de gestión.
- Facilitar el seguimiento preventivo a riesgos críticos y riesgos residuales.
- Apoyar la toma de decisiones para la implementación de acciones de tratamiento, mitigación o fortalecimiento de controles.
- Fortalecer la cultura de monitoreo y mejora continua en la gestión institucional del riesgo.

Gradualidad de implementación

La implementación de Indicadores Clave de Riesgo (KRI) en la entidad se realizará de

forma gradual, priorizando procesos y riesgos que, por su impacto, probabilidad o nivel residual, requieran mecanismos reforzados de seguimiento preventivo, en los riesgos clasificados como altos, extremos o críticos, con alta recurrencia, materialización histórica o impacto significativo sobre los objetivos institucionales, así como aquellos asociados a procesos considerados críticos para la operación institucional.

La entidad podrá establecer mecanismos diferenciales de monitoreo conforme a la naturaleza y criticidad de los riesgos identificados.

Los criterios técnicos, mecanismos de monitoreo, parámetros, periodicidades, fuentes de información, responsables operativos, umbrales de seguimiento y demás elementos requeridos para la definición e implementación de Indicadores Clave de Riesgo (KRI) serán desarrollados mediante instrumentos metodológicos, lineamientos técnicos, matrices o herramientas complementarias adoptadas por la entidad para la gestión y monitoreo de riesgos.

La implementación integral de los KRI se realizara de manera progresiva conforme a las capacidades y necesidades institucionales de monitoreo.

Corresponderá a las líneas de defensa en el marco de sus competencias y responsabilidades institucionales, la identificación, monitoreo y reporte de los Indicadores Clave de Riesgo (KRI), así:

La primera línea de defensa identifica y reportar la información requerida para el monitoreo de los riesgos y de los KRI asociados a sus procesos.

La segunda línea de defensa brinda lineamientos metodológicos, acompañamiento técnico y consolidación institucional de la información relacionada con el monitoreo de riesgos y KRI.

La tercera línea de defensa, en ejercicio de sus funciones de evaluación independiente, verificará la efectividad de los mecanismos de monitoreo implementados y formulará recomendaciones de mejora cuando corresponda.

18.2 Lineamientos de Seguimiento para los Riesgos de Integridad Pública

Aunque los riesgos de integridad pública deben incluirse dentro de los informes periódicos de seguimiento, su naturaleza crítica exige condiciones especiales de monitoreo, trazabilidad y control. Esta categoría incluye los riesgos de corrupción, fraude, soborno, conflicto de interés y lavado de activos, financiación del terrorismo y proliferación de armas de destrucción masiva (LA/FT/FPADM).

18.3 Procedimiento para la ejecución de controles:

El primer paso fundamental consiste en desarrollar un inventario exhaustivo y sistemático de todos los controles existentes en el mapa de riesgos, lo cual implica identificar y documentar detalladamente cada control activo, incluyendo su propósito, responsable, frecuencia de ejecución y el riesgo específico que busca mitigar. Este proceso debe comenzar con una recopilación de información a través de reuniones con los dueños de procesos, revisión de documentación existente y validación de procedimientos actuales, asegurándose de registrar cada control en una matriz estructurada que incluya elementos como el código identificador único, nombre descriptivo, tipo de control (preventivo, detectivo o correctivo), estado actual, última fecha de revisión, responsables tanto de ejecución como de supervisión, proceso al que pertenece. Es crucial que esta actividad inicial se realice de manera metódica y detallada, ya que servirá como base fundamental para todas las actividades subsecuentes del proceso de gestión y control de riesgos, permitiendo establecer un punto de referencia claro para el seguimiento y la evaluación futura de la efectividad de los controles, es necesario realizar una evaluación detallada de la efectividad y funcionamiento de cada control identificado realizando:

Tabla 41 Ejecución de controles
Fuente: Ministerio De Igualdad y Equidad

Luego de completar el análisis de los controles existentes, el siguiente paso consiste en desarrollar e implementar un plan de acción integral que aborde todas las deficiencias y oportunidades de mejora identificadas. Este plan debe incluir acciones correctivas específicas con responsables claramente designados, plazos de implementación realistas, recursos necesarios y métricas de seguimiento definidas. Es fundamental proceder con el rediseño de controles inefectivos, la creación de nuevos controles donde se identificaron brechas, la actualización de procedimientos y documentación relacionada, así como la implementación de mejoras cuando sea necesario. Todo esto debe ir acompañado de un proceso robusto de comunicación y capacitación para el personal involucrado, seguido por un de monitoreo continuo que incluya revisiones periódicas, evaluaciones de efectividad y actualizaciones de las matrices de riesgo y control. Esta fase es crucial para asegurar que las mejoras implementadas realmente fortalezcan el sistema de control de riesgos de la organización.

El monitoreo a los mapas de riesgos, *la realizará los Líderes de Proceso*, con el apoyo de los gestores, de acuerdo con la periodicidad establecida en la Política de Administración de Riesgos y las responsabilidades establecidas.

18.4 Lineamientos para la modificación de controles ante cambios en

procesos

En el marco del seguimiento y monitoreo continuo al Sistema de Gestión de Riesgos, cuando se identifica una modificación o cambio en alguno de los procesos institucionales que pueda afectar la efectividad de los controles establecidos (sean estos riesgos de gestión, corrupción, seguridad digital, o de cualquier otra naturaleza), es fundamental implementar un procedimiento sistemático y documentado que permita actualizar, fortalecer y adaptar las medidas de control existentes. Este procedimiento busca garantizar que los cambios en los procesos no generen vulnerabilidades, Incrementan la probabilidad de materialización de riesgos, asegurando así la continuidad y efectividad de las operaciones institucionales. A continuación, se detallan los pasos a seguir cuando se detecta una modificación en los procesos que requieren ajustes en los controles de riesgos:

RESPONSABLES

- Líderes de proceso
- Oficina de Planeación
- Comité Institucional de Coordinación de Control Interno
- Gestores de Riesgo designados

PROCEDIMIENTO

1. Identificación del Cambio

Responsable: Líder del Proceso

- Documentar la modificación identificada en el proceso
- Evaluar el impacto preliminar sobre los controles existentes
- Notificar a la Oficina de Planeación sobre los cambios detectados

2. Análisis del Impacto

Responsable: Oficina Asesora de Planeación y Líder del proceso

- Realizar mesa de trabajo para evaluar el impacto del cambio.
- Identificar controles afectados
- Evaluar la efectividad actual de los controles
- Determinar la necesidad de nuevos controles.

- Diseñar nuevos controles si se requieren
- Definir recursos necesarios
- Establecer cronograma de implementación

3. Aprobación

Responsable: Comité Institucional de Coordinación de Control Interno

- Presentar propuesta de codificación Evaluar viabilidad de cambios Aprobar o solicitar ajustes

4. Implementación

Responsable: Líder del Proceso

- Socializar cambios aprobados
- Actualizar documentación del proceso
- Capacitar al personal involucrado
- Implementar nuevos controles
- Registrador de evidencias de implementación

5. Seguimiento

Responsable: Oficina Asesora de Planeación

- Verificar implementación de cambios
- Evaluar efectividad de nuevos controles
- Generar informe de seguimiento
- Proponer ajustes si se requieren

19. PRESENTACIÓN DEL INFORME DE GESTIÓN DE RIESGOS POR LA SEGUNDA LÍNEA DE DEFENSA

La Oficina Asesora de Planeación, como segunda línea de defensa del Sistema, tiene la responsabilidad de consolidar y presentar el informe de gestión de riesgos con el propósito de facilitar la toma de decisiones estratégicas basadas en una evaluación

integral del Sistema. De la Gestión de Riesgos institucionales. A continuación, se detallan las responsabilidades y características fundamentales de este proceso:

- Recopila información de la primera línea (líderes de proceso)
- Incorporar resultados del monitoreo periódico.
- Valida datos con las áreas responsables
- Analiza tendencias y patrones
- Recomendaciones
- Primera Línea: Proporciona información sobre la ejecución de controles
- Tercera Línea (Control Interno): Informe de resultados de evaluaciones independientes

Contenido del informe:

- Estado general de la gestión de riesgos
- Nivel de cumplimiento de controles
- Riesgos materializados
- Efectividad de los controles
- Recomendaciones de mejora

Este informe constituye una herramienta fundamental para la toma de decisiones estratégicas y el fortalecimiento continuo del Sistema de Gestión de Riesgos institucional.

20. SEGUIMIENTO A LOS MAPAS DE RIESGOS

La Oficina de Planeación, será quien apoye a la entidad, en el seguimiento periódico a los Planes de Manejo establecidos en los Mapas de Riesgos de gestión, fiscal y de integridad publica y los Planes de Manejo de los riesgos de Seguridad de la información se hará acorde con las roles y responsabilidades dadas al responsable de seguridad de la información del Ministerio.

El Grupo Interno de Trabajo de Control Interno del Ministerio o quien hace sus veces, a través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación o quien haga sus veces. (Guía Administración Riesgos V.6 DAFP)

21. LINEAMIENTOS PARA LA SEGREGACIÓN DE FUNCIONES EN PROCESOS CRÍTICOS

La segregación de funciones constituye un control transversal determinante en el Sistema de Gestión de Riesgos del Ministerio de Igualdad y Equidad, actuando como barrera preventiva frente a posibles eventos de riesgo operativo, fraude o corrupción. Este principio, fundamentado en la Ley 87 de 1993 y alineado con la Guía de Administración del Riesgo del DAFP, representa una clave de control para mitigar los riesgos inherentes en procesos críticos, especialmente aquellos relacionados con el manejo de recursos públicos, toma de decisiones y custodia de bienes. La adecuada segregación de funciones reduce la probabilidad de materialización de riesgos al evitar la concentración de funciones incompatibles en un mismo servidor público, fortaleciendo así las tres líneas de defensa del Sistema de Control Interno. El Ministerio, en su compromiso con una gestión efectiva del riesgo, establece los siguientes lineamientos normativos y recomendaciones prácticas para implementar y mantener una segregación de funciones que contribuya eficazmente al tratamiento de riesgos institucionales.

22. CONTROL Y SEGUIMIENTO A LOS RIESGOS

Los líderes responsables como primera línea de defensa ejercerán un monitoreo continuo y permanente sobre los riesgos de sus procesos, como parte inherente de su gestión diaria. La Oficina Asesora de Planeación, como segunda línea de defensa, solicitará cuatrimestralmente las evidencias del seguimiento realizado para consolidar el estado de la gestión del riesgo institucional. Las fechas establecidas para este seguimiento se detallan en el numeral 25 del presente documento.

La Oficina de Control Interno como tercera línea de defensa evalúa de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos y los que inadecuadamente son cubiertos por la 2ª línea de defensa. A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces se garantiza el cumplimento efectivo de los objetivos.

22.1 Reporte resultado del monitoreo y seguimiento

Cuando el análisis o los resultados del seguimiento realizado por el Grupo Interno de Control Interno o los entes de control determinen la necesidad de modificar los mapas de riesgo, el responsable del proceso deberá analizar los hallazgos identificados y revisarlos conjuntamente con su equipo, quienes por su conocimiento y cercanía al proceso están en mejor condición de valorar el impacto real de los cambios. Una vez surtido este análisis interno, se reportará a la Oficina de Planeación para actualizar los componentes correspondientes: riesgos, causas, consecuencias, controles o planes de manejo.

Los reportes se realizarán mediante correo electrónico con soporte en la Matriz de Riesgos; para riesgos de Seguridad de la Información, la comunicación se dirigirá a la Oficina de Tecnologías de la Información con copia al responsable de seguridad digital.

22.2 Función de Cumplimiento

La función de cumplimiento es una obligación legal establecida en la Ley 2195 de 2022 (artículo 31) y reglamentada por el Decreto 1122 de 2024, que exige a las entidades públicas prevenir, gestionar y administrar riesgos de:

Lavado de activos, financiación del terrorismo y proliferación de armas (LA/FT/FP)
Corrupción en todas sus formas
Reporte de operaciones sospechosas ante la UIAF y la Fiscalía

Es el eje central del **SIGRIP** (Sistema de Gestión de Riesgos para la Integridad Pública), sin el cual la entidad no puede demostrar operación íntegra ante la ley.

RESPONSABILIDADES[3]

1. Operación y supervisión del SIGRIP

Velar por el funcionamiento efectivo, eficiente y oportuno de todo el sistema, apoyando a los líderes de proceso y gestores de riesgo.

2. Evaluación periódica y reporte a la Alta Dirección

Presentar resultados de gestión, reportes de operaciones y planes de mejoramiento en la periodicidad definida institucionalmente.

3. Revisión y adopción de lineamientos normativos

Revisar y recomendar la implementación de directrices del DAFP, Secretaría de Transparencia, UIAF y entidades de control en materia de riesgo.

4. Mejora continua del SIGRIP

Promover y adoptar correctivos, y proponer a la Alta Dirección la actualización de elementos del sistema.

5. Coordinación interinstitucional y capacitación

Articular con dependencias internas la operatividad del SIGRIP y gestionar programas

[3] Guia para la gestión integral de riesgos v7,DAFP Bogotá 2025 disponible en
https://www.funcionpublica.gov.co/documents/d/guest/2025-09-11_guia_gestion_integral_riesgo_v7?download=true

de capacitación en cumplimiento y gestión de riesgos.

6. Diseño de metodologías e indicadores

Colaborar en el diseño y aplicación de modelos cualitativos y cuantitativos que requiera el sistema.

7. Debida diligencia en conocimiento de contrapartes

Establecer lineamientos para aplicar mecanismos proporcionales de conocimiento de proveedores, contratistas y terceros.

8. Gestión de operaciones inusuales y sospechosas

Elaborar criterios para identificar operaciones inusuales y sospechosas, y someterlos a aprobación de la Alta Dirección.

9. Reporte a autoridades competentes

Reportar a la UIAF, Fiscalía General de la Nación u otra autoridad competente las operaciones intentadas o sospechosas identificadas.

La función de cumplimiento **no reemplaza ni restringe** las funciones de la Unidad de Control Interno.

23. SOCIALIZACIÓN Y COMUNICACIÓN

La comunicación y divulgación de la política y la metodología para la administración de los riesgos, será dada a conocer por la Oficina de Planeación, en coordinación con la Oficina de Comunicaciones, la cual se realizará a través de los diferentes
medios de comunicación interna, con el fin de dar cubrimiento al mayor número de servidores públicos de la Entidad, tanto a nivel central, como a nivel territorial.

Así mismo, los líderes de proceso con el apoyo de los gestores socializarán la política y los mapas de riesgos a los equipos de trabajo, así como los cambios y actualizaciones que se llegarán a generar, dejando registro de estas.

24. FECHAS DE SEGUIMIENTOS Y PUBLICACIÓN

El seguimiento se realiza tres (3) veces al año, así:

Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.

Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10), primeros días hábiles del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero"[13]**.**

Para el seguimiento de los riesgos de corrupción, se podrá utilizar el formato del Anexo 6 Matriz de seguimiento a los riesgos de corrupción de la Guía del DAFP.

25. CONTROL DE CAMBIOS

Cuando se requiera modificar o actualizar la Política de Administración de Riesgos, en relación con la política, la metodología para la gestión de riesgos, lo realizará la Oficina de Planeación y se presentará en el Comité Institucional de Coordinación Control Interno, para ser aprobado por parte del Representante Legal Ministerio de conformidad con el literal g del artículo 2.2.21.1.6 del Decreto 1083 de 2015. (Funciones del Comité).

Versión	Fecha	Descripción del cambio	Responsable
1.0	03/12/2024	Versión inicial de la Política de Administración de Riesgos: Proporciona un marco integral y sistemático para la gestión de riesgos dentro del Ministerio de la Igualdad y Equidad	Jefe Oficina Asesora de Planeación
2.0	05/06/2026	En la versión 2 de la Política de Riesgos se realizaron las siguientes actualizaciones y fortalecimientos: • **Controles:** Se actualizó y reforzó el marco de controles institucionales • **Materialización de riesgos:** Se amplió el tratamiento y protocolo de gestión • **Seguridad de la información:** Se incorporó integralmente el componente de seguridad de la información	Jefe Oficina Asesora de Planeación

		• **Actualización normativa:** Se alineó con el nuevo Manual de Riesgos SIGRIP V7 2025 En el marco de la actualización a la versión 7 de la Guía para la Gestión Integral de Riesgos, se realizó la revisión y actualización de la presente política, incorporando herramientas e instrumentos orientados a la prevención, detección y respuesta frente a riesgos de corrupción, fraude, soborno, lavado de activos, financiación del terrorismo, conflictos de interés e incumplimientos al código de integridad, así como lineamientos clave en materia de integridad pública, riesgos fiscales y seguridad de la información. Lo anterior, en alineación con el Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP–, con el propósito de fortalecer la capacidad institucional para identificar, analizar, valorar y gestionar de manera integral los eventos que puedan afectar el ejercicio íntegro del servicio público y la confianza ciudadana en la institución.	

Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta"

La actualización, modificación, ajuste y publicación de la Política estará a cargo de la Oficina de Planeación y se publicará con las versiones actualizadas en el repositorio y en la página web de la Entidad en el enlace de transparencia. Las modificaciones o actualización de versiones a la política, sus anexos y formatos para la gestión de riesgos, que no impliquen cambios en la política y metodología serán realizadas por la Oficina de Planeación, cuando así se requiera y publicadas con las versiones actualizadas, en el repositorio y en la página web de la Entidad en el enlace de transparencia

26. FORMALIZACIÓN

	Elaboró técnica y metodológicamente	Revisó	Aprobó
Nombre y Apellido	Amparo Orozco Molina Cesar Lizarazo	Luis Gabriel Espitia Pinzón	Julian Alfredo Medica Cadena

Cargo	Profesional Oficina Asesora de Planeación Contratista	Profesional Especializado Grado 17 Oficina Asesora de Planeación	Jefe de Oficina Oficina Asesora de Planeación (E)