MANUAL PARA LA GESTIÓN INTEGRAL DEL RIESGO

Versión:002
Unidad de Planeación de Infraestructura de Transporte
Grupo Interno de Trabajo de Planeación
Bogotá D.C., julio de 2026

CONTENIDO

1. Introducción 5
2. Objetivo 6
3. Alcance 6
4. Glosario 6
5. Siglas: 11
6. Normatividad Aplicable 11
7. Documentos externos requeridos 12
8. Documentos internos requeridos 12
9. Políticas de Operación para la Administración del Riesgo 12
9.1. Roles y Responsabilidades Frente a la Administración Integral del Riesgo en la UPIT 15
Línea Estratégica – Alta Dirección 15
9.2. Primera Línea – Líderes de Proceso y sus equipos de trabajo 17
9.3. Segunda Línea – Responsables de Seguimiento y Gestión del Riesgo 18
9.4. Tercera Línea – Asesor Control Interno 19
10. Política para la gestión integral de riesgos 20
10.1. Niveles de flexibilidad de la UPIT ante los riesgos. 21
10.1.1. Apetito diferenciado por tipología y tolerancia cero frente a la corrupción 22
9.2 Articulación para la gestión integral de riesgos 23
9.3 Análisis del contexto interno y externo 23
9.4 Riesgos Generales de la Gestión Institucional 24
10.Identificación y descripción del riesgo 25
10.1 Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados: 25
Identificación de áreas de impacto de los riesgos 25
Identificación de áreas de factores de riesgo 25
Descripción del riesgo 27
Causas inmediatas para los riesgos de integridad pública 30
10.2 Paso 2. Análisis de riesgo inherente 30
Determinación del impacto inherente 32

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Análisis de Severidad 33
10.3 Paso 3. Diseño y Análisis de Controles 35
Estructura para la redacción de Controles 36
Tipología de controles (Atributos de eficiencia) 38
Valoración de controles 39
10.4 Paso 4. Valoración del Riesgo Residual 40
Estrategias para combatir los riesgos 41
10.5 Acciones de fortalecimiento de los controles 42
Cómo redactar las acciones de fortalecimiento 42
Formulación, periodo de cobertura y cumplimiento 43
Parametrización y seguimiento en la herramienta para la implementación del sistema de gestión dispuesto por la Entidad. 43
11. Gestión de Riesgos Fiscales 47
12. Riesgos De Seguridad De La Información 49
a. Identificación de los activos de información: 50
b. Clasificación Del Activo De Información (ISO 27001) 52
c. Índice De Información Clasificada Y Reservada 54
d. Datos Personales (Ley 1581 De 2012) 55
e. Aprobación de la Identificación, Clasificación y valoración de Activos 56
f. Proceso De Gestión De Riesgos De Seguridad De La Información 58
i. Amenazas y Vulnerabilidades 59
ii. Descripción del riesgo 61
iii. Determinar la probabilidad 62
iv. Determinación del Impacto 63
v. Estructura para la Descripción del Control 65
vi. Valoración de Controles 65
vii. Atributos 65
g. Valoración Del Riesgo Residual 67
h. Plan de implementación de controles 67
13. Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP 68

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Amenazas para la integridad pública 68

Soborno 68

Fraude 69

Inadecuada gestión del conflicto de intereses: 69

Corrupción 70

Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP 70

14. Sistema de Gestión del Riesgo 70

14.1 Operación del SIGRIP 71

14.2 Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos 72

Opciones de tratamiento 77

Focos de riesgo para la integridad propios de la UPIT 77

Debida diligencia en el conocimiento de las contrapartes 78

Flujo de reporte de operaciones inusuales y sospechosas 78

Función de cumplimiento 79

Canal de denuncias y protección al denunciante 79

15. Indicadores Clave de Riesgo 80

Tipologías de Indicadores para el seguimiento 80

Alcance de los Indicadores Claves de Proceso y los Indicadores Clave de Riesgo . 81

16. Conclusión 84

17. Bibliografía 86

18. Anexos (Cuando aplique) 87

19. Control de documentos 88

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

1. Introducción

En el desarrollo de sus funciones misionales y administrativas, la Unidad de Planeación de Infraestructura de Transporte — en adelante UPIT se encuentra expuesta a diferentes situaciones internas y externas que pueden afectar el cumplimiento de sus objetivos institucionales, la adecuada prestación de sus servicios, la toma de decisiones y la generación de valor público. Por esta razón, la administración del riesgo constituye una herramienta fundamental para anticipar, prevenir, controlar y mitigar aquellos eventos que puedan impactar negativamente la gestión institucional.

El Modelo Integrado de Planeación y Gestión — MIPG establece, en el marco de la Política de Planeación Institucional, la necesidad de que las entidades públicas definan lineamientos claros para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos. En este sentido, la gestión del riesgo permite fortalecer la planeación, mejorar los controles, orientar la toma de decisiones y contribuir al logro de los resultados previstos por la entidad.

El Departamento Administrativo de la Función Pública — DAFP, mediante la séptima versión de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, actualizó la metodología para la gestión de riesgos en el sector público, consolidando una estructura común para su administración, independientemente de su naturaleza. Esta actualización incorpora elementos del marco internacional COSO-ERM 2017, tales como el apetito de riesgo y los niveles de madurez, los cuales permiten fortalecer la capacidad institucional para gestionar los riesgos de manera integral y sistemática.

Así mismo, la Guía V7 incorpora el Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP, como marco teórico y metodológico orientado a la identificación, análisis, tratamiento y seguimiento de los riesgos que puedan afectar la ética, la transparencia, la legalidad y la integridad pública. En particular, el Capítulo VI de dicha guía establece lineamientos específicos relacionados con el análisis del contexto de integridad, la identificación de vulnerabilidades institucionales y el fortalecimiento de una cultura organizacional basada en la integridad pública.

En atención a estos lineamientos, la UPIT actualiza su instrumento para la Administración de Riesgos, con el propósito de adaptar las orientaciones emitidas por el DAFP a su modelo de operación por procesos, fortalecer la gestión preventiva, mejorar el diseño y seguimiento de controles, e incorporar el componente SIGRIP como parte integral de la administración de riesgos institucionales.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Este documento busca orientar a los procesos de la entidad en la adecuada gestión de sus riesgos, promoviendo una cultura institucional basada en la prevención, el autocontrol, la transparencia, la mejora continua y la integridad pública, en procura del cumplimiento de los objetivos estratégicos y del fortalecimiento de la confianza ciudadana en la gestión de la UPIT.

2. Objetivo

Establecer los lineamientos estratégicos, metodológicos y operativos para la identificación, análisis, valoración, tratamiento, monitoreo, revisión, comunicación y seguimiento de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales y la integridad pública en la Unidad de Planeación de Infraestructura de Transporte — UPIT, en concordancia con el Modelo Integrado de Planeación y Gestión, las mejores prácticas internacionales de gestión de riesgos basadas en el marco de COSO -ERM y los lineamientos definidos por el DAFP.

3. Alcance

La política desarrollada en el presente manual aplica a todas las dependencias, procesos, funcionarios y contratistas de la Entidad, en todos los niveles jerárquicos. Incluye los lineamientos para el tratamiento de riesgos de gestión, riesgos fiscales, riesgos contra la integridad pública y riesgos de seguridad de la información.

4. Glosario

Definiciones:

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Apetito de 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.

Beneficiario final: persona natural que finalmente posee o controla a una contraparte o en cuyo nombre se realiza una operación.

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

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

y bienes fiscales, definidos así: a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc. b) 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.

Canal de denuncias: mecanismo dispuesto por la Entidad para recibir, evaluar, tramitar y cerrar denuncias o inquietudes asociadas a corrupción o a conductas contrarias a la integridad pública, con protección al denunciante.

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.

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.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

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. Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.

Contraparte: persona natural o jurídica con la que la Entidad establece una relación contractual, comercial, interinstitucional o de cualquier otra índole (proveedores, contratistas, consultores, aliados o beneficiarios).

Control: Medida que permite reducir o mitigar un riesgo.

Debida diligencia: conjunto de procedimientos, políticas y gestiones mediante los cuales la Entidad conoce adecuadamente a sus contrapartes, verifica su identidad, evalúa su historial y consulta listas restrictivas, antes y durante la relación.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

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

Eventos: Tratándose de riesgos de gestión, corrupción y fiscales un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad. En cuanto a riesgos de seguridad de la información un evento es la ocurrencia o cambio de un conjunto particular de circunstancias. (Existen muchos eventos a nivel de elementos de tecnología, ejemplo: Encender, Apagar, Login de usuario, Cierre de sesión). Los eventos de seguridad de la información pueden indicar una posible brecha de seguridad de la información o falla de un control.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Función de cumplimiento: rol responsable de la dirección, coordinación y vigilancia del adecuado funcionamiento del SIGRIP y de cada uno de sus componentes.

Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique) . A título de ejemplo son gestores fiscales, entre otros, sin perjuicio de las particularidades de cada entidad: representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

Gestor público: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros, sin perjuicio de las particularidades de cada entidad: los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Gobernanza: Es la forma en la que se organizan los diferentes actores para tomar decisiones y resolver problemas comunes; en el contexto de la administración de riesgos, hace referencia a los ajustes institucionales y de control que aseguran que los riesgos sean conocidos, comunicados, gestionados y monitoreados en toda la entidad.

Incidentes: En seguridad de la información, son eventos inesperados que tienen probabilidad significativa de comprometer las operaciones del negocio.

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

Inherente: Característica de una cosa que hace que por su naturaleza este inseparablemente unido a otra.

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.

Operación inusual: operación cuya cuantía o características no guardan relación con la actividad o el comportamiento esperado de la contraparte o del segmento y que, por ello, es objeto de análisis.

Operación sospechosa: operación inusual que, una vez analizada, no encuentra justificación razonable y que debe reportarse a las autoridades competentes.

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07).

Persona Expuesta Políticamente (PEP): persona que ejerce o ha ejercido funciones públicas prominentes y respecto de la cual se aplica debida diligencia reforzada.

Probabilidad: se entiende 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.

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Recurso público: Para efectos del capítulo de riesgos fiscales, 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: Probabilidad de que se genere un efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

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

Riesgo de Seguridad de la Información: 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 27000).

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.

Seguridad de la información: busca proteger la información independientemente del medio en que se encuentre mediante la confidencialidad, integridad y disponibilidad.

Seguridad digital: Acorde con la política de Gobierno Digital y los lineamientos del MSPI, busca gestionar los riesgos asociados al entorno digital completo:

– Seguridad de la información,
– Seguridad informática,
– Ciberseguridad.
– Protección de infraestructuras críticas.
– Gestión de incidentes digitales.
– Continuidad de servicios digitales.
– Protección de servicios ciudadanos digitales.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Señal de alerta: criterio o parámetro que advierte sobre posibles operaciones inusuales y orienta su detección y análisis.

Soborno: Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directa o indirectamente, e independientemente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una parte actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.

Tolerancia del riesgo: Diferencia entre el nivel de apetito / aceptación de riesgo y el nivel máximo admisible de riesgo definido en la entidad.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. Siglas:

CICCI: Comité Institucional de Coordinación de Control Interno

CIGD: Comité Institucional de Gestión y Desempeño

DAFP: Departamento Administrativo de la Función Pública.

LA: Lavado de Activos

FT: Financiación del Terrorismo

FP: Financiamiento de la Proliferación de Armas de Destrucción Masiva

MIPG: Modelo Integrado de Planeación y Gestión

SIGRIP: Sistema de Gestión de Riesgos para la Integridad Pública

UPIT: Unidad de Planeación de Infraestructura de Transporte

6. Normatividad Aplicable

La Normatividad que regula este procedimiento o las citas normativas que se enuncian en las actividades, se encuentra definidas en el Normograma de la UPIT, disponible para consulta en el siguiente link al normograma.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

7. Documentos externos requeridos

Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 6 diciembre de 2024 – Departamento Administrativo de la Función Pública Función Pública – DAFP.

Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 agosto de 2025 – Departamento Administrativo de la Función Pública Función Pública – DAFP.

Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional Abril de 2025 - Ministerio de Tecnologías de la Información y las Comunicaciones.

8. Documentos internos requeridos

La documentación interna que hace parte de este documento se encuentra definida en el Banco de Documentos de la UPIT en el siguiente link: Banco de documentos 2.0.xlsx

9. Políticas de Operación para la Administración del Riesgo

Con el fin de contar con una herramienta útil que le permita a la UPIT un aseguramiento razonable respecto al logro de sus objetivos, además de los lineamientos ya enunciados, se adoptan las siguientes políticas de operación, las cuales recogen y hacen exigibles los desarrollos metodológicos contenidos en el presente manual (apetito de riesgo, líneas, riesgos fiscales, riesgos de seguridad de la información, SIGRIP, monitoreo y mejora). Estas políticas son de obligatorio cumplimiento para todas las dependencias, procesos, funcionarios y contratistas de la Entidad, en todos los niveles jerárquicos.

- La Política para la Gestión Integral de Riesgos es única y transversal. Una misma política y metodología rigen la gestión de todas las tipologías de riesgo de la Entidad (gestión, fiscales, seguridad de la información e integridad pública), evitando esquemas paralelos o desarticulados.
- La Política para la Gestión Integral de Riesgos debe ser aprobada por el Comité Institucional de Coordinación de Control Interno – CICCI.
- El presente manual y su metodología se revisan y/o actualizarán por lo menos una vez al año, o cada vez que se presenten cambios normativos, ajustes en la plataforma estratégica, en el modelo de operación por procesos o en el contexto interno y externo que originen nuevos riesgos o modifiquen los existentes.
- Los roles y responsabilidades del esquema de líneas son de aplicación obligatoria y guardan segregación de funciones: primera línea identifica y

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

gestiona, la segunda línea acompaña y consolida, y la tercera línea evalúa de forma independiente.

- La Alta Dirección, a través del CIGD, debe garantizar los recursos humanos y tecnológicos necesarios para la adecuada administración de los riesgos, incluyendo el talento humano idóneo, las herramientas de formulación y seguimiento, y los espacios de almacenamiento de las evidencias de control.
- La única documentación válida en materia de administración del riesgo es la publicada en el Banco de Documentos de la UPIT; cualquier otra copia se considera copia no controlada.
- La UPIT acepta únicamente los riesgos que, después de su análisis y valoración, se ubiquen en zona de severidad baja (verde). Los riesgos que se ubiquen en zonas moderada, alta o extrema deben ser objeto de tratamiento para llevarlos a niveles tolerables.
- Las estrategias para combatir el riesgo (aceptar, reducir, transferir o evitar) deben definirse a partir de la zona en que quede ubicado el riesgo residual; la transferencia mediante seguros o tercerización no traslada la responsabilidad reputacional ni la titularidad pública del riesgo.
- Los controles deben atacar las causas raíz y los factores de riesgo identificados, redactarse con la estructura y atributos definidos en el manual, y diseñarse de manera que su valoración no sobreestime la mitigación (especialmente los controles correctivos).
- La Entidad debe evaluar periódicamente su nivel de madurez para la gestión del riesgo con base en el modelo COSO-ERM, y la segunda línea presentará a la Alta Dirección las acciones de mejora que de allí se deriven.
- Los mapas de riesgos se elaboran y administran en la herramienta para la implementación del sistema de gestión de la entidad, manteniendo la coherencia con el esquema metodológico del presente manual; la consolidación del mapa de riesgos institucional está a cargo del GIT de Planeación.
- La primera línea (líderes de proceso) realiza monitoreo cuatrimestral a sus riesgos, con corte al último día hábil de diciembre, abril y agosto, reportando estado y evidencias de los controles, avance del plan de tratamiento y materialización de riesgos en la herramienta para la implementación del sistema de gestión de la entidad conforme a las fechas definidas por el GIT de Planeación.
- La segunda línea (GIT de Planeación) realiza la evaluación de la gestión del riesgo dentro de los diez (10) días hábiles de los meses de mayo, septiembre y enero, y presenta sus resultados al Comité Institucional de Gestión y Desempeño.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- La tercera línea (Asesor de Control Interno) ejecuta una evaluación independiente al diseño y ejecución de los controles basada en riesgos, conforme la planeación del Plan Anual de Auditoría, priorizando los procesos de mayor exposición y registrando las no conformidades a que haya lugar.
- Las evidencias de la aplicación de los controles deben conservarse y custodiarse de forma trazable durante los términos legales aplicables, asegurando su disponibilidad para las labores de evaluación y auditoría.
- El Control Fiscal Interno es responsabilidad de todos los servidores públicos y particulares que administren recursos, bienes o intereses patrimoniales de naturaleza pública, en especial de los gestores fiscales (ordenadores y ejecutores del gasto, pagadores, supervisores, estructuradores y responsables de la planeación contractual, entre otros).
- La descripción del riesgo fiscal debe diferenciar la causa raíz (hecho generador) del efecto dañoso, y no confundir el riesgo fiscal con el daño patrimonial ni con la determinación de responsabilidades, que corresponde a los órganos de control fiscal.
- Cada proceso debe identificar, clasificar y valorar sus activos de información conforme a los lineamientos del MSPI del MinTIC, registrando criticidad en términos de confidencialidad, integridad y disponibilidad.
- La Entidad debe gestionar de forma integral los riesgos para la integridad pública (soborno, fraude, inadecuada gestión del conflicto de intereses, corrupción y LA/FT/FP), articulados con los riesgos de gestión, fiscales y de seguridad de la información.
- Toda operación intentada, inusual o sospechosa de LA/FT/FP debe reportarse a las autoridades competentes (Unidad de Información y Análisis Financiero – UIAF y/o Fiscalía General de la Nación), con independencia de que se configure o no el delito.
- Las herramientas, la política y el mapa de riesgos del SIGRIP hacen parte integral del Programa de Transparencia y Ética Pública, y la información y registros de las contrapartes y sus operaciones deben conservarse por el término del artículo 12 de la Ley 2195 de 2022.
- La materialización de un riesgo para la integridad pública no implica prejuzgamiento ni responsabilidad, y la respuesta institucional debe orientarse a asegurar la continuidad del servicio y de la operación de la Entidad.
- La Entidad debe adelantar acciones permanentes de formación y toma de conciencia sobre el SIGRIP y la gestión integral del riesgo, dirigidas a funcionarios, contratistas y líderes de proceso, incluyendo objetivos, elementos, beneficios e implicaciones del incumplimiento.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Los líderes de proceso deben socializar con sus equipos los riesgos y controles identificados, garantizando su comprensión y correcta aplicación en la operación diaria.
- Cuando los procesos realicen el monitoreo deben indicar si se materializó o no el riesgo. En caso de que se materialice realizar las acciones descritas en el capítulo relacionado con este.

9.1. Roles y Responsabilidades Frente a la Administración Integral del Riesgo en la UPIT

Línea Estratégica – Alta Dirección

Con el fin de garantizar una operación articulada y una adecuada gestión de los riesgos, La UPIT cuenta con el Comité Institucional de Gestión y Desempeño - CIGD reglamentado a través de la Resolución 036 de 2025, el cual es el órgano orientador, articulador y ejecutor, a nivel institucional, de las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento del Modelo Integrado de Planeación y Gestión – MIPG en la Unidad de Planeación de Infraestructura de Transporte – UPIT[1].

Por otra parte, en la Entidad se cuenta con el Comité Institucional de Coordinación de Control Interno – CICCI; reglamentado a través de la Resolución 096 de 2022, el cual está conformado como un órgano de asesoría y coordinación en los asuntos del sistema de control interno de la Unidad.[2]

Estas dos instancias componen la línea estratégica en la UPIT y tendrán los siguientes roles en la Administración de los Riesgos:

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

El Comité analiza la gestión del riesgo y define mejoras al MIPG con énfasis en las actividades de control establecidas en todos los niveles de la organización, estudiando y adoptando las mejoras propuestas por el CICCI.

EL CIGD aprueba las directrices para la administración del riesgo en la Entidad y es el responsable del fortalecimiento de la política de administración del riesgo en la Unidad, el comité debe:

---

[1] Unidad de Planeación de Infraestructura de Transporte [UPIT]. (2025, 03 de marzo). *Por la cual se crea el Comité Institucional de Gestión y Desempeño de la Unidad de Planeación de Infraestructura de Transporte – UPIT, se establece su reglamento y se dictan otras disposiciones* [Resolución 036 de 2025]. Art. 2.

[2] Unidad de Planeación de Infraestructura de Transporte [UPIT]. (2022, 01 de diciembre). *Por medio de la cual se integra y adopta la reglamentación del Comité Institucional de Coordinación del Sistema de Control Inteno de la Unidad de Planeación de Infraestructura de Transporte – UPIT [*Resolución 096 de 2022]. Art. 1.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Velar por que en la Entidad se disponga de los recursos necesarios para la adecuada administración de los riesgos
- Revisar y aprobar el contexto estratégico, la plataforma estratégica, el modelo de operación por procesos y la planeación institucional, con el propósito de identificar cambios que puedan originar nuevos riesgos o modificar los existentes.
- Aprobar y hacer seguimiento a las acciones y estrategias adoptadas para la operación del MIPG, lo que implica entre otros, aprobar la política de administración del riego de la entidad y propiciar su actualización periódica.
- Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del MIPG, lo que conlleva también, incorporar dentro de la planeación estratégica el análisis de riesgos para decidir respecto de los objetivos, las metas y niveles de riesgo aceptados y no aceptados en su consecución.
- Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión, lo que requiere establecer los mecanismos y responsables de monitorear el desempeño los resultados de la gestión de riesgos y compartir en dicha instancia estos resultados para la definición de las acciones estratégicas y/o de mejora, consecuentes.
- Analizar las evaluaciones de la gestión del riesgo, elaboradas por la Segunda y Tercera Línea y tomar las decisiones a las que haya lugar.
- Analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.

COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO

El Comité aprueba la Política de Administración del Riesgo; analiza los eventos y riesgos críticos haciendo seguimiento en especial a la prevención y detección de fraude y mala conducta.

Así mismo le corresponde:

- Evaluar el estado del Sistema de Control Interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del sistema.
- Aprobar el Plan Anual de Auditoría de la entidad, hacer sugerencias y seguimiento a las recomendaciones, con el fin de asegurar que su alcance y recursos faciliten la cobertura de los proyectos estratégicos de la entidad, así como la priorización de las unidades auditables críticas para la misma, según la priorización y el análisis de riesgos hecho por la Asesoría de Control Interno de la UPIT.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Evaluar la aplicación de las acciones de contingencia en los casos en que se presenta la materialización de un riesgo.
- Aprobar la Política para la gestión del riesgo de la Entidad con todos sus componentes.
- Verificar que el esquema de líneas atiende de manera íntegra la gestión del riesgo al interior de la entidad, comprometiendo todos los niveles de la organización.
- Analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.

9.2. Primera Línea – Líderes de Proceso y sus equipos de trabajo

Compuesta por servidores y contratistas en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad, se encarga del mantenimiento efectivo y correcta aplicación de los controles definidos; por consiguiente, identifica, evalúa, controla y mitiga los riesgos.

LÍDERES DE PROCESOS

Los líderes de proceso tienen la responsabilidad de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se divulguen a cada servidor público y/o contratista involucrado en el proceso, es importante recordar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

Adicionalmente, la primera línea debe:

- Evaluar los cambios que se presenten en la plataforma estratégica de la entidad o en su contexto estratégico, analizando cómo estos cambios originan nuevos riesgos o modifican los ya existentes.
- Liderar la identificación de los riesgos del proceso a cargo, siguiendo los lineamientos establecidos en el Manual para la Administración del Riesgo de la UPIT
- Realizar, con el apoyo de su grupo de trabajo, la gestión y administración de los riesgos identificados.
- Realizar la evaluación de la formulación y la solidez de los controles, para determinar la pertinencia y la necesidad de ajuste o modificación, en caso de presentarse.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Adelantar la revisión, actualización periódica y seguimiento de los mapas de riesgos, y si es el caso ajustarlos.
- Establecer controles que contribuyan a mitigar riesgos del proceso.
- Socializar los controles implementados con su equipo de trabajo, con el fin de asegurar que sean comprendidos por todos, garantizando su correcta y oportuna aplicación.
- Monitorear constantemente la correcta aplicación de los controles
- Analizar los eventos de materialización de los riesgos y aplicar los lineamientos que se definan para su adecuada gestión.
- Realizar la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.

FUNCIONARIOS Y CONTRATISTAS

- Participar en la construcción y administración de los riesgos del proceso dentro del cual ejercen sus funciones o desarrollan sus labores.
- Conocer los riesgos asociados al proceso al cual pertenecen, así como los riesgos de la Entidad.
- Ejecutar los controles operativos y acciones definidas para la administración de los riesgos definidos y aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

9.3. Segunda Línea – Responsables de Seguimiento y Gestión del Riesgo

GRUPO INTERNO DE TRABAJO DE PLANEACIÓN– PROCESO SISTEMA INTEGRADO DE GESTIÓN

- Construir la metodología para la administración del riesgo en la UPIT, de acuerdo con la normatividad y los lineamientos establecidos para cada una de las tipologías, a excepción de aquellas tipologías que requieren un desarrollo metodológico particular por su naturaleza, tales como: los riesgos ambientales, de seguridad y salud en el trabajo y seguridad de la información, riesgos de contratación, etc.
- Adelantar el seguimiento de los mapas de riesgos, evaluando la eficacia en la implementación de los controles, generando recomendaciones y posibles ajustes a los mapas de riesgos de los procesos.
- Realizar ejercicios de asesoría y acompañamiento a los líderes de los procesos y sus equipos para la mejora en la implementación de la metodología.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Consolidar y publicar el mapa de riesgos institucional y de corrupción.
- Presentar los resultados del seguimiento y evaluación de los mapas de riesgos al Comité Institucional de Gestión y Desempeño.
- En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP asume la función de cumplimiento que se desarrolla en el capítulo Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP del presente documento.

GRUPO INTERNO DE TRABAJO DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones – proceso Gestión de Tecnologías de la Información es responsable de validar e implementar la metodología para la identificación y gestión de riesgos de seguridad digital, la cual hace parte integral de este documento y que se desarrolla de acuerdo con los lineamientos establecidos por el Ministerio de las TIC.

Así mismo es responsable de adelantar el seguimiento de los mapas de riesgos de seguridad digital, evaluando la eficacia en la implementación de los controles, generando recomendaciones y posibles ajustes a los mapas de riesgos de seguridad digital de los procesos.

9.4. Tercera Línea – Asesor Control Interno

- Establecer el plan anual de auditoría basado en riesgos, priorizando aquellos procesos de mayor exposición, así como la verificación del funcionamiento de los componentes de control interno.
- Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.
- Evaluar la efectividad de la Gestión del Riesgo en la Entidad a través de la verificación de la adecuado diseño y aplicación de controles y su aporte en la mitigación de los riesgos identificados.
- Adelantar el registro de no conformidades, en el marco de las auditorías internas, cuando se constituya un incumplimiento en la aplicación de la política de riesgo.
- Acompañar y asesorar metodológicamente a los procesos, en la administración y gestión integral de riesgos, en coordinación con la segunda línea.
- Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Comunicar al Comité de Coordinación de Control Interno posibles cambios evidenciados en la evaluación del riesgo, detectados durante las auditorías.
- Alertar a la alta dirección sobre la probabilidad de materialización de riesgos en las dependencias y procesos auditados.

10. Política para la gestión integral de riesgos

De conformidad con las directrices establecidas en la *Guía para la Gestión Integral del Riesgo en Entidades Públicas versión7 de 2025*, la UPIT adopta el presente documento como el marco de referencia que establece las líneas de acción para la gestión del riesgo en la Unidad.

La política de administración del riesgo es la declaración e intención general que hace la UPIT respecto a la gestión y administración de sus riesgos, por lo anterior se compromete a:

> "*La Unidad de Planeación de Infraestructura de Transporte – UPIT bajo el liderazgo de la alta dirección, gestionará integralmente sus riesgos con base en los lineamientos establecidos en el Manual para Gestión Integral del Riesgo M-SIG-022 vigente o el que haga sus veces, el cual establece las directrices precisas para su tratamiento, manejo y seguimiento; buscando así evitar y/o mitigar las consecuencias en caso de materialización, mediante actividades de prevención, sensibilización y control de tal manera que pueda garantizar el cumplimiento de sus objetivos institucionales con una cultura de prevención y mitigación del Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP).*"

Como parte de la Política para la Gestión Integral del Riesgo, y en el marco del SIGRIP, la Entidad formula una política institucional que expresamente:

- Manifiesta el compromiso de la Alta Dirección con una cultura de prevención y mitigación del Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP).
- Prohíbe y rechaza cualquier práctica asociada al LA/FT/FP.
- Obliga a la Entidad a cumplir con la normativa Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP).

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

10.1. Niveles de flexibilidad de la UPIT ante los riesgos.

Entendiendo que la administración de los riesgos es un ejercicio dinámico que en la UPIT se ha venido consolidando consistentemente con la implementación de la metodología definida, se hace necesario precisar los niveles o límites de riesgos que en la Entidad podría soportar sin llegar a arriesgar el cumplimiento de sus objetivos ni comprometer la eficiencia operativa.

Para poder determinar dichos niveles es necesario primero definir los siguientes conceptos:

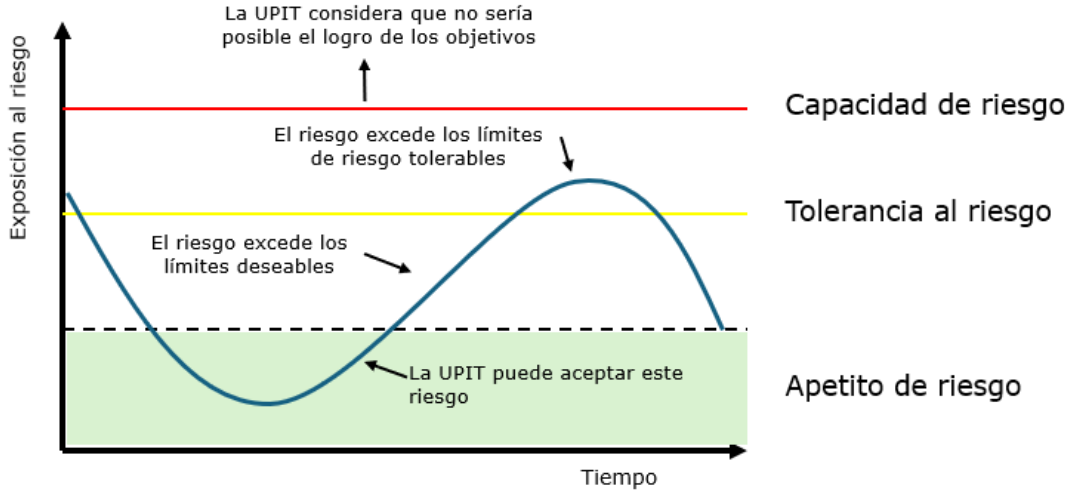
Aceptación del riesgo: Entendido como el nivel de riesgo que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. En la UPIT se aceptan aquellos riesgos que, después de su análisis y valoración, se ubiquen en el nivel de riesgo bajo, identificado por el color verde dentro del mapa de calor.

Tolerancia del riesgo: Entendido como el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor de aceptación del riesgo (apetito) determinado por la entidad. Esto es, el nivel en donde el riesgo excede el límite aceptable en la Entidad, pero aun así la entidad puede garantizar el cumplimiento de sus objetivos.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que la UPIT puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos planteados.

Gráficamente, la flexibilidad de la UPIT ante los riesgos se puede observar en la siguiente imagen:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA



Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

En la UPIT, cada nivel conlleva el desarrollo de acciones con diferentes prioridades y en horizontes de tiempo diversos.

10.1.1. Apetito diferenciado por tipología y tolerancia cero frente a la corrupción

El apetito de riesgo puede ser diferente según la tipología de riesgo que la Entidad gestiona. Como regla general, la UPIT acepta los riesgos que, después de su valoración, se ubican en zona de severidad baja (verde).

No obstante, frente a los riesgos de corrupción y demás riesgos para la integridad pública la UPIT define una tolerancia cero: con independencia de la zona en que se ubique el riesgo residual, estos riesgos siempre son objeto de tratamiento y no pueden ser aceptados. De igual forma, frente a los riesgos de LA/FT/FP, toda operación inusual o sospechosa, incluso la intentada, debe analizarse y reportarse, sin que su no materialización justifique la inacción.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Matriz de Tolerancia del riesgo en la UPIT

NIVEL DE RIESGO	PRIORIDAD	PLAN DE MITIGACIÓN
EXTREMO	Requiere el desarrollo de acciones inmediatas con reportes continuos a la Alta Dirección por parte del líder del proceso	Planes de tratamiento enfocados a disminuir la exposicion de la Unidad a este riesgo, su probabilidad e impacto
ALTO	Requiere planes de tratamiento urgentes con reportes periodicos al líder del proceso	Requiere la ejecución de actividades para disminuir la exposicion del riesgo como transferencias a terceros, cobertura de seguros o acciones que disminuyan la probabilidad y/o el impacto
MODERADO	Acciones con prioridad moderada, pudiendo ejecutarse en el mediano plazo	Desarrollar acciones encaminadas a desarrollar nuevos controles o a fortalecer los existentes
BAJO	Riesgo aceptable, se mitiga con los controles rutinarios	No se requieren acciones de control adicionales a las ya establecidas



9.2 Articulación para la gestión integral de riesgos

Con el fin de lograr una administración eficaz de aquellas situaciones que la UPIT identifique como posibles riesgos que puedan afectar el cumplimiento de sus funciones y objetivos institucionales, los cuales involucra la afectación al patrimonio público (riesgos fiscales), la posible vulneración a activos de información, así como la afectación a la confianza de las múltiples partes interesadas en el uso del entorno digital (Riesgos de Seguridad de la Información) y aquellas conductas asociadas a comportamientos no éticos que van en contravía del ejercicio íntegro del servicio público (Riesgos contra la Integridad), es necesario definir elementos comunes como el análisis del contexto estratégico interno y externo, la definición de la política para la gestión integral del riesgo y los pasos metodológicos aplicables de **i) identificación y descripción del riesgo, ii) análisis del riesgo inherente, iii) diseño y análisis de controles y iv) valoración del riesgo residual**.

9.3 Análisis del contexto interno y externo

Con anterioridad a la identificación de los riesgos, cada proceso, con el acompañamiento del GIT de Planeación, analiza el contexto en el que opera la Entidad como insumo para reconocer las fuentes de riesgo y, en particular, las vulnerabilidades para la integridad pública. Este análisis se actualiza por lo menos una vez al año y cuando se presenten cambios relevantes en el entorno o en la operación.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

El análisis del contexto comprende, como mínimo:

- **Contexto externo:** factores políticos, económicos, sociales, tecnológicos, ambientales y legales; partes interesadas del sector transporte; y entorno de corrupción y de LA/FT/FP que pueda afectar a la Entidad.
- **Contexto interno:** plataforma estratégica, modelo de operación por procesos, estructura, talento humano, recursos tecnológicos y cultura organizacional.
- **Contexto del proceso:** objetivo, actividades clave, productos o servicios y puntos de la cadena de valor donde se genera exposición al riesgo.
- **Vulnerabilidades para la integridad:** condiciones internas que podrían facilitar el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción o el LA/FT/FP.

9.4 Riesgos Generales de la Gestión Institucional

En este apartado, se desarrollarán los pasos requeridos para la identificación; el análisis, el diseño de controles y la valoración del riesgo residual, para los riesgos asociados a la operación de la entidad también conocidos como **Riesgos de Gestión**; sin embargo, estos pasos son transversales y deben realizarse también para los ***Riesgos Fiscales y Riesgos para la Integridad Pública.***

A continuación, se presenta el esquema de pasos que se deben seguir para la correcta gestión de riesgos.

Pasos para la Administración de los Riesgos



Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

10.Identificación y descripción del riesgo

10.1 Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados:

Lo anterior aplica para los ***Riesgos de Gestión****,* ***Riesgos Fiscales y Riesgos para la Integridad Pública.***

Para una identificación asertiva y precisa de los riesgos claves de cada proceso, deberán considerarse aquellos eventos que podrían afectar de forma previsible el logro de sus objetivos, considerados y ya formulados. De igual manera, en la herramienta para la implementación del sistema de gestión de la entidad se parametrizará todo el ciclo y flujo de los riesgos por parte del GIT de Planeación.

De este modo, para establecer los puntos de riesgo clave en los procesos, es necesario considerar además del objetivo, el ciclo del proceso y también los atributos de los productos, servicios o resultados de procesos que podrían verse afectados, así como el efecto de estos posibles eventos en el resultado de otros procesos, dentro de una misma cadena de valor.

Para llevar a cabo este análisis se utiliza la **caracterización del proceso,** en donde además del objetivo, se debe considerar la estructura de este con sus ***actividades clave*** y demás componentes dentro del ciclo de los procesos, los cuales se resumen a continuación.

Identificación de áreas de impacto de los riesgos

Si bien los riesgos pueden afectar diferentes áreas en la Entidad, la metodología para la administración de los riesgos del Departamento Administrativo de la Función Pública – DAFP adoptada en la UPIT, establece el área de impacto como la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo.

En otras palabras, el impacto de la materialización de un riesgo en la UPIT podrá ser ***económico (presupuestal) y/o reputacional.***

Identificación de áreas de factores de riesgo

Los factores de riesgo, en términos generales, hacen referencia a las fuentes en donde se pueden originar 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.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

A continuación, como una guía, se establece un listado con los factores de riesgo que pueden incidir en un proceso, no obstante, las dependencias o procesos de acuerdo con su particularidad pueden identificar otras situaciones o fuentes.

FACTOR	DEFINICIÓN	DESCRIPTORES
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Ausencia de procedimientos o falta de aplicación de los existentes
		Falta segregación de funciones
		Errores de grabación, autorización
		Falta de supervisión o interventoría
		Errores en cálculos para pagos internos y externos
		Alta rotación o insuficiencia de personal
		Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
		Acciones contrarias a las leyes o acuerdos contractuales
		Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP	Eventos relacionados con transacciones y operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la entidad (naturales o jurídicas)
		Productos (bienes o servicios) que oferta/requiere
		Canales utilizados para la operación
		Jurisdicciones (nacional o territorial
Talento humano	Eventos relacionados con las conductas o comportamientos de los funcionarios o contratistas que afectan la Integridad Pública	Fraude Interno
		Soborno
		Gestión inadecuada de conflicto de Intereses
		Corrupción
		Hurto de activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de sistemas de información y aplicaciones Hackeo de los sistemas de la entidad
		Caída de redes
		Errores en hardware o software
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

		Daños a activos fijos
Evento Externo	Eventos por situaciones externas que afectan la entidad	Fraude Externo
		Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

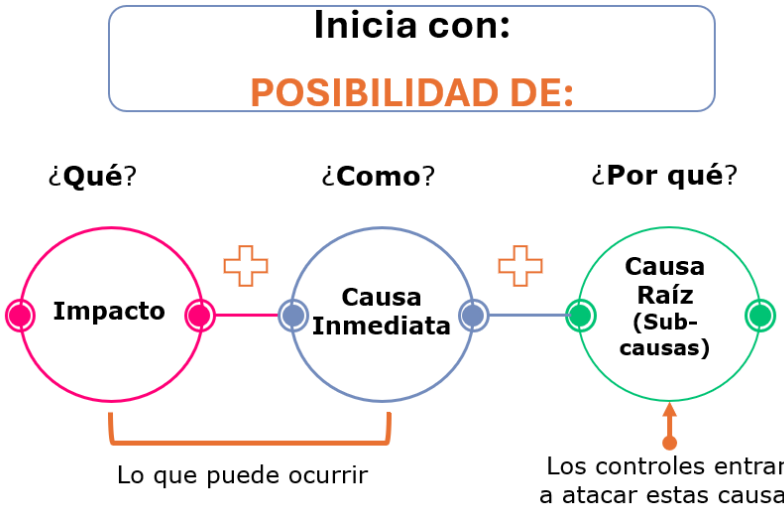
La importancia de la definición o identificación de los factores de riesgos se basa en que, una vez la entidad haya reconocido esas situaciones que pueden aumentar la probabilidad de que algo salga mal, en un ejercicio preventivo puede empezar a generar herramientas que ayuden a contrarrestar o evitar que se presenten las situaciones riesgosas; de esta manera, la identificación de los factores de riesgo se convierte en el primer paso para una correcta definición de causas y la creación de controles asertivos .

Descripción del riesgo

Una vez identificados los puntos de riesgos claves, área de impacto y factores de riesgo se debe proceder con la descripción del riesgo; detallando los aspectos necesarios para su identificación. En la herramienta para la implementación del sistema de gestión de la entidad se parametrizará todo el ciclo y flujo de los riesgos.

En la UPIT, la descripción de los riesgos se debe realizar aplicando la siguiente estructura:

Estructura para la redacción del riesgo



Fuente: Elaboración propia a partir de Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Desglosando cada uno de los componentes de la estructura propuesta tenemos:

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.

Características clave del riesgo al momento de su descripción es que debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar.

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, información esencial para la definición de controles en el apartado de diseño y análisis de controles. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Un adecuado análisis de causa raíz debe permitir diferenciar la causa raíz, de la causa inmediata, entendida esta última como las circunstancias más evidentes sobre las cuales se presenta el riesgo y que en ocasiones, no constituyen la causa principal del riesgo.

Lo anterior aplica para los Riesgos de Gestión, Riesgos Fiscales, Riesgos para la Integridad Pública y Riesgos de Seguridad de la Información.

Ejemplo:

Proceso: Relacionamiento con la ciudadanía

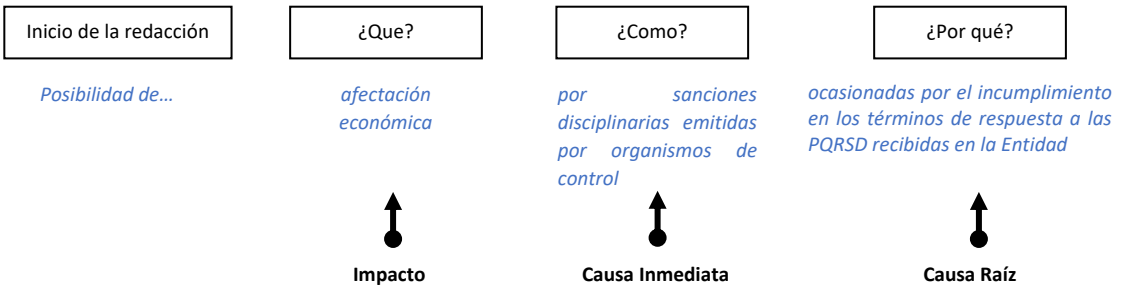
Objetivo: Definir, orientar y promover lineamientos para la debida prestación del servicio al ciudadano, la participación y la atención de las PQRS dentro de los términos de ley, haciendo seguimiento a las respuestas de los requerimientos de los peticionarios, buscando medir y mejorar la percepción de buena atención y la satisfacción de los grupos de valor

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Actividades clave: Se identifica como una de las actividades clave del proceso el "*la atención de las PQRS dentro de los términos de ley, haciendo seguimiento a las respuestas de los requerimientos de los peticionarios*"

Una vez identificada una de las actividades claves del proceso, se identifican aquellos eventos que podrían ocasionar que el proceso no cumpla con su objetivo.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:



Fuente: Elaboración propia a partir de Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025

A continuación, se presentan unos ejemplos que puede adoptar la UPIT frente a la identificación de riesgos de integridad pública.

Posibilidad de afectación reputacional y económica **por corrupción** en la priorización de proyectos de infraestructura de transporte, a causa de la modificación injustificada de criterios técnicos, sociales o económicos para favorecer un proyecto, territorio, actor político o tercero interesado.
Posibilidad de afectación económica **por conflicto de intereses** en la formulación del plan de inversiones del sector transporte, a causa de la participación de servidores o contratistas con vínculos personales, familiares o económicos con beneficiarios directos de los proyectos priorizados.
Posibilidad de afectación económica y operativa **por fraude interno** en la elaboración o revisión de estudios de prefactibilidad, a causa de la inclusión de datos inexactos de demanda, costos, tráfico, accidentalidad o beneficio social para justificar la viabilidad de un proyecto.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Causas inmediatas para los riesgos de integridad pública

Para los riesgos de integridad pública, la *Guía para la Gestión Integral del Riesgo en Entidades Públicas versión7 de 2025*, reconoce como causas inmediatas o manifestaciones principales:

Causa inmediata	Uso recomendado
Corrupción	Cuando se desvían recursos, decisiones o gestión administrativa para beneficio propio o de terceros.
Fraude interno	Cuando hay errores, omisiones, informes inexactos o manipulaciones con culpa o dolo para beneficio personal o de terceros.
Fraude Externo	Se define como toda pérdida, daño o afectación institucional derivada de actos de fraude cometidos por **terceros o personas ajenas a la organización**. En este tipo de evento, no participa ningún funcionario, contratista o miembro interno de la entidad.
Soborno entrante	Cuando se acepta o solicita una ventaja indebida.
Soborno saliente	Cuando se ofrece, promete o entrega una ventaja indebida.
Conflicto de interés	Cuando se decide o participa en asuntos donde existe interés particular, familiar, económico o de terceros.
LA/FT/FP	Cuando la entidad puede ser utilizada para dar apariencia de legalidad a activos ilícitos o canalizar recursos hacia terrorismo o proliferación de armas.

Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

10.2 Paso 2. Análisis de riesgo inherente

Una vez identificados y descritos los riesgos, se procede a analizar su nivel inherente, entendido como la valoración del riesgo antes de considerar la aplicación de controles. Este análisis se realiza a partir de la determinación de la probabilidad

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

de ocurrencia y del impacto que podría generar su materialización, con el propósito de establecer el nivel de exposición inicial del proceso y orientar posteriormente la definición o fortalecimiento de los controles correspondientes.

Los criterios señalados en este apartado aplican a los riesgos de gestión, riesgos fiscales y riesgos para la integridad pública.

Determinación de la probabilidad inherente

Para efectos de este análisis, la probabilidad de ocurrencia de un riesgo estará asociada a la exposición al riesgo del proceso o la actividad que se esté analizando. De este modo, *la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año*.

Con este esquema se busca que "*la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.*"[3]

Así las cosas, la exposición al riesgo estará asociado al proceso o actividad que se esté analizando, es decir, *al número de veces que se realiza la actividad que genera el riesgo en el periodo de 1 año*, en la siguiente tabla, se establecen los criterios para definir el nivel de probabilidad de ocurrencia de un riesgo en la UPIT.

Criterios para definir el nivel de probabilidad

Probabilidad	Frecuencia de la Actividad	% Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces al año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año	60%

[3] *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Alta	La actividad que conlleva el riesgo se ejecuta mínimo 501 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de la entidad, bajo las cuales se definen las escalas de probabilidad:

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Actividades asociadas a la Planeación estratégica de la Unidad.	1 vez al año	Muy Baja
Actividades de gestión del talento humano, gestión jurídica, gestión administrativa.	Mensual (12 veces por año)	Media
Actividades asociadas a Tecnología (disponibilidad de aplicativos, protocolos de seguridad informática)	Diaria (Mas de 500 en el año)	Alta
Radicación de documentos recibidos y enviados por la Entidad	Diaria (Mas de 5000 al año)	Muy Alta

Determinación del impacto inherente

Tal como se identificó en la página 26 del apartado de Identificación de áreas de impacto de los riesgos del presente manual; para la UPIT el impacto de la materialización de un riesgo será *económico o reputacional.*

La afectación económica hace referencia al deterioro económico que sufrirían las finanzas de la entidad producto de situaciones adversas como, por ejemplo; pagos por sentencias en su contra, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal, etc.

Por su parte, la afectación reputacional hace referencia al desgaste o pérdida de credibilidad, confianza y legitimidad que puede sufrir la Entidad ante sus grupos de interés (ciudadanía, entes de control, otras instituciones y medios de comunicación).

En general, cuando se habla de impacto, se refiere a las *consecuencias* que puede ocasionar a la entidad la materialización de un riesgo; para lograr cuantificar el

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

impacto que tendría la materialización de un riesgo, se cuenta con la tabla de criterios que define tanto los impactos económicos como los reputacionales

Criterios para definir el nivel de impacto

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

Fuente: *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

Cuando se considere que el riesgo tendrá un impacto tanto económico como reputacional y al hacer la medición presentan diferentes niveles de impacto, se debe tomar el nivel más alto, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, en este caso se toma el nivel moderado, como el nivel de impacto del riesgo

Análisis de Severidad

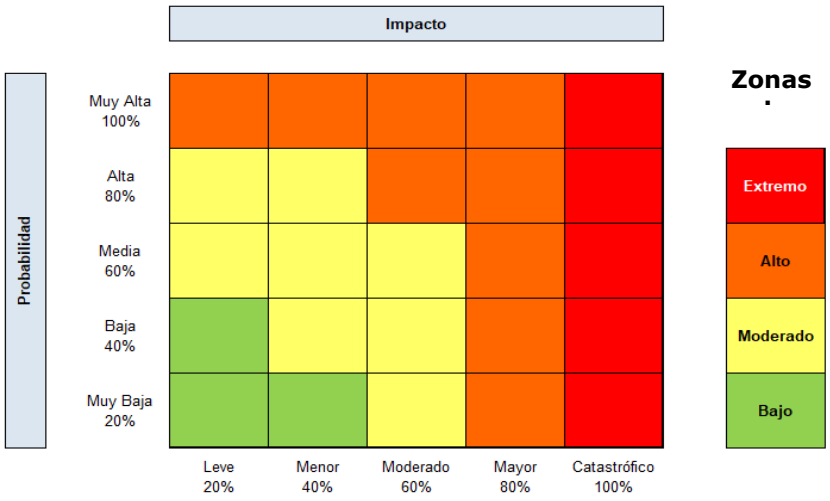
Una vez establecidas la probabilidad de ocurrencia y el impacto potencial del riesgo, se procede a determinar su nivel de severidad inherente. Este análisis permite establecer el grado de exposición del proceso antes de considerar la aplicación de controles y constituye la base para definir las medidas de tratamiento correspondientes.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Los criterios señalados en este apartado aplican a los riesgos de gestión, riesgos fiscales y riesgos para la integridad pública.

El nivel de severidad se obtiene mediante la combinación de la probabilidad de ocurrencia y el impacto que tendría la materialización del riesgo sobre el proceso. El resultado del cruce de estas dos variables se representa en una matriz de calor conformada por cuatro (4) zonas de severidad: baja, moderada, alta y extrema, como se observa en la siguiente tabla.

Matriz de Calor para Análisis de la Severidad



Fuente: *Elaboración propia*

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar el nivel de **RIESGO INHERENTE**.

Ejemplo

Proceso: Relacionamiento con la Ciudadanía

Objetivo: Definir, orientar y promover lineamientos para la debida prestación del servicio al ciudadano, la participación y la atención de las PQRS dentro de los términos de ley, haciendo seguimiento a las respuestas de los requerimientos de los peticionarios, buscando medir y mejorar la percepción de buena atención y la satisfacción de los grupos de valor

Riesgo Identificado: Posibilidad de afectación económica por sanciones disciplinarias emitidas por organismos de control ocasionadas por el incumplimiento en los términos de respuesta a las PQRSD recibidas en la Entidad

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

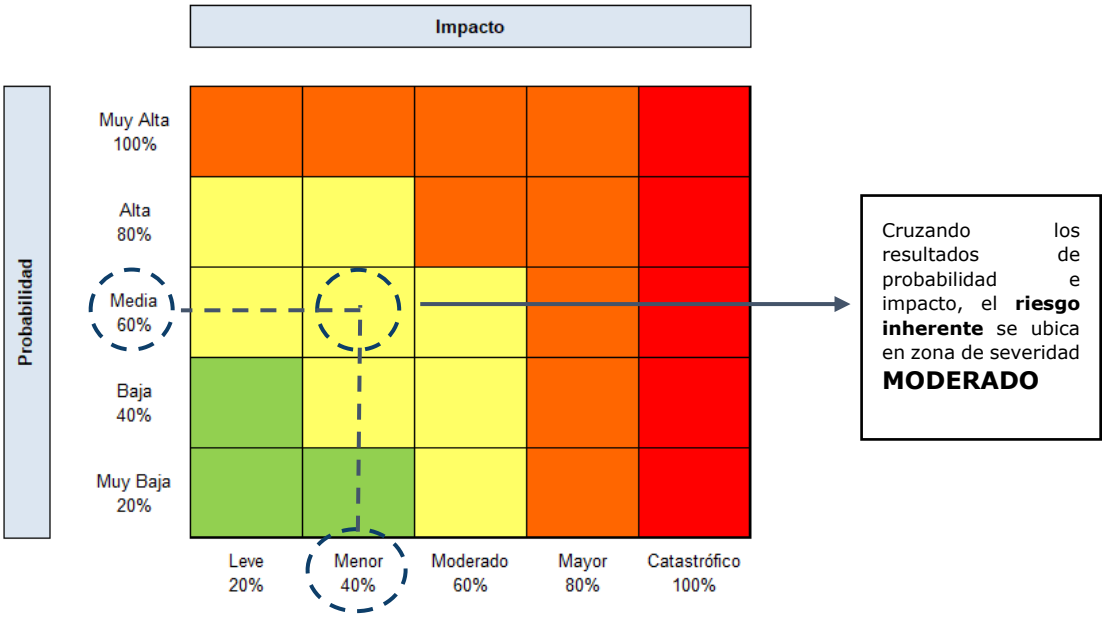
Luego del análisis realizado por el proceso se determinó que, para establecer la probabilidad, se tiene en cuenta el número de PQRS recibidas en la vigencia anterior, en este caso 436; aplicando los criterios para la determinación de la probabilidad, se ubica en probabilidad MEDIA ya que "*La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año*".

Probabilidad Inherente: MEDIA (60%)

En cuanto al impacto, el proceso determinó que "el riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y/o de proveedores" por lo tanto se determina que el impacto inherente es Menor

Impacto Inherente: MENOR (40%)

Aplicando los datos en la matriz de calor tenemos:



10.3 Paso 3. Diseño y Análisis de Controles

*Lo anterior aplica para los Riesgos de Gestión, Riesgos Fiscales y Riesgos para la Integridad Pública.

Los controles o 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

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

ofrecer una seguridad razonable respecto al logro de los objetivos. Para la identificación o bien el diseño de controles se debe tener en cuenta que:

- 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.

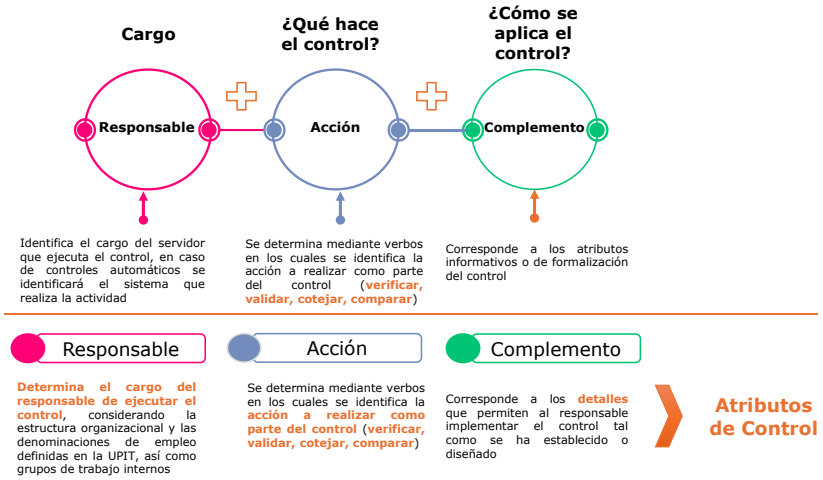
- Se requiere considerar los diferentes atributos de las actividades de control para asegurar aspectos tales como: los responsables de su ejecución, la segregación de funciones y niveles de autoridad apropiados.

- 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.

Estructura para la redacción de Controles

Para un adecuado diseño de las actividades de control se propone la siguiente estructura para su redacción, la cual agrupa los atributos necesarios para garantizar su implementación de forma efectiva por parte del responsable:

Estructura para la redacción de controles



Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Desglosando los atributos para el control tenemos:

Responsable: Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (directores, asesores, profesionales, técnicos, asistenciales, coordinadores, contratistas, etc.).

Cuando se trate de controles automáticos realizados por sistemas de información, se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.

Acción: Determina para qué se realiza el control, se utilizar verbos fuertes como: revisar, verificar, confrontar, comparar, cotejar, detectar, analizar etc.

Atributos Informativos o de formalización del control: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos:

✓ **Documentación**: se refiere a la fuente documental de los controles, bien sea que su definición y forma de aplicarlo esté documentada en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.

✓ **Frecuencia**: corresponde a la periodicidad con la cual se ejecuta una actividad de control; debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente (puede ser periódica o por evento).

✓ **Evidencia**: permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.

✓ **Ejecución**: permite establecer cómo se ejecuta el control, por lo general, las acciones de control se desarrollan a través de actividades en donde se compara o verifica el cumplimiento de criterios previamente definidos; así, se debe definir qué acciones se toman en caso de desviaciones o situaciones que se detecten.

Aplicando todos los atributos anteriormente descritos, los controles se constituyen en una herramienta efectiva.

Ejemplo

Proceso: Relacionamiento con la Ciudadanía

Control Definido:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Responsable	Frecuencia de Aplicación	Acción de control	Complemento
El profesional especializado ubicado en la Secretaría General - Servicio al Ciudadano	diariamente	revisa en el gestor documental las pqrsd con tiempos próximos a vencer	en caso de identificar un solicitud que esté a 3 días o menos para su vencimiento, emite una alerta por correo electrónico al funcionario y/o contratista que tiene asignado la gestión de la pqrsd, solicitando que tome las acciones pertinentes para su respuesta en los términos de ley. Como evidencia queda el correo electrónico enviado al responsable

Tipología de controles (Atributos de eficiencia)

Lo anterior aplica para los Riesgos de Gestión, Riesgos Fiscales y Riesgos para la Integridad Pública.

Los tipos de controles se dividen en dos; de acuerdo con su orientación y de acuerdo con la forma en que se ejecutan. Cada uno de estos tipos cuentan con sus propios atributos de eficiencia para mitigar los riesgos y sus causas en mayor o menor medida.

Teniendo en cuenta la orientación del control, existen tres tipos; controles preventivos, detectivos o correctivos, o bien una combinación de estos.

Esta orientación se puede entender desde el ciclo de procesos, con el fin de establecer el momento en que se activa el control en función de las actividades claves del proceso:

Control preventivo: control ***accionado en la entrada del proceso*** y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Las políticas de operación son un buen ejemplo de un control preventivo.

Control detectivo: control ***accionado durante la ejecución del proceso***. Estos controles detectan el riesgo, pero generan reprocesos. Los puntos de control dentro de los procedimientos, generalmente, son controles detectivos

Control correctivo: control ***accionado en la salida del proceso*** y después de que se materializa el riesgo. Estos controles tienen costos implícitos. se implementan de forma preventiva, es decir requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización, pero no pueden clasificarse como preventivos, ya que sería una sobrevaloración de control que podría generar análisis errados en los niveles de severidad. En consecuencia, si bien estos controles requieren en su diseño que se apliquen actividades con un enfoque preventivo, al ser activados al momento de materialización del riesgo deben ser considerados como controles correctivos no preventivos. Un ejemplo de este

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

tipo de controles usualmente tiene que ver con pólizas de seguro, copias de seguridad (*backup*), bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez se materializa.

De acuerdo con la forma en que se ejecutan los controles, estos pueden ser:

Controles Manuales: Ejecutados por personas

Controles automáticos: Ejecutados por un sistema o software previamente programado o diseñado

Valoración de controles

Los atributos de eficiencia de los controles, inciden directamente en su efectividad; en la siguiente tabla, se analizan estos atributos para determinar en qué porcentaje el control contribuye a mitigar el riesgo y sus causas.

Tabla de valoración de controles

Características			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 pueden 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 automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%

Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

Ahora bien, la estructura de redacción de controles y los atributos informativos que se desarrollaron en el presente documento, son muy importantes al momento de redactar un control, sin embargo, no tienen una incidencia directa en su efectividad.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

10.4 Paso 4. Valoración del Riesgo Residual

*Aplica para los Riesgos de Gestión, Riesgos Fiscales y Riesgos para la Integridad Pública.

El riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que, estos 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.
Para mayor claridad, en la siguiente tabla, se observan los cálculos requeridos para la aplicación de dos (2) controles, uno preventivo y uno detectivo.

Este ejercicio es la continuación del ejemplo que se viene desarrollando en el presente documento con un caso aterrizado a la realidad de la Unidad de Planeación de Infraestructura de Transporte – UPIT.

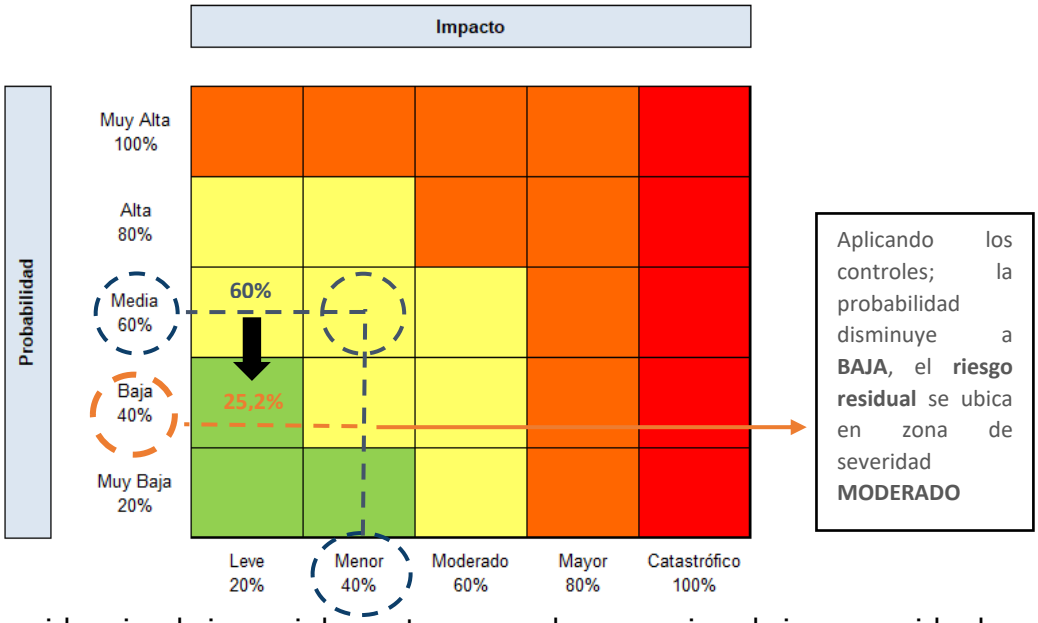
Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
Posibilidad de afectación económica por sanciones disciplinarias emitidas por organismos de control ocasionadas por el incumplimiento en los términos de respuesta a las PQRSD recibidas en la Entidad	Probabilidad Inherente	**60%**	Valoración control 1 (preventivo)	**40%**	60% X 40%=24% 60%-24%= **36%**
	Valor probabilidad para aplicar segundo control				**36%**
	Valoración control 2 (detectivo)			**30%**	36% X 30%=10,8% 36%-10,8%= **25,2%**
	Probabilidad Residual				**25,2%**
	Valoración de Impacto				
	Impacto Inherente	**40%**	No se tienen controles para aplicar al impacto		
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual				**40%**

Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Gráficamente, en la matriz de calor se evidencia el efecto de la aplicación del control en la disminución de la zona de severidad:



En color azul se evidencia el riesgo inherente y en color naranja, el riesgo residual, es decir después de la aplicación de los controles.

Una vez aplicada la totalidad de la metodología explicada se procede con la elaboración de los mapas de riesgo por proceso, cuya estructura es definida por el Grupo Interno de Trabajo de Planeación a través de una herramienta para la implementación del sistema de gestión de la entidad, el cual mantiene la misma línea del esquema metodológico propuesto en el presente documento.

Estrategias para combatir los riesgos

Aplica para los Riesgos de Gestión, Riesgos Fiscales y Riesgos para la Integridad Pública.

Las estrategias para combatir el riesgo son las acciones que el proceso debe emprender para mitigar el riesgo. Estas acciones y la urgencia de su implementación dependerán de la zona en donde se encuentre ubicado el riesgo residual.

Si después de evaluar los controles el riesgo se ubica en zona de riesgo BAJO, se puede determinar *asumir el riesgo*, conociendo los efectos de su posible materialización. Asumir el riesgo significa que se deben seguir aplicando los controles implementados y mantener las acciones de monitorización sobre el control.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Si después de evaluar los controles definidos por el proceso para el riesgo aún permanece en zona de riesgo MODERADO, ALTO o EXTREMO, se sugiere una estrategia para ***Reducir el riesgo***, es decir; implementar acciones[4] que ayuden a fortalecer los controles (aumentar su calificación en la evaluación) o desarrollar acciones nuevas con el fin de evaluar si eventualmente pueden ser consideradas como nuevos controles que ayuden a disminuir la probabilidad o el impacto. (Acciones de Fortalecimiento).

Si después de realizar un análisis, se considera que la mejor estrategia es ***transferir el riesgo***, es decir tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se trasfiere la responsabilidad sobre el tema reputacional

Sí después de realizar un análisis se considera que el riesgo es demasiado alto, se puede determinar **evitar el riesgo**, es decir, no asumir la actividad que genera el riesgo o cambiar la forma de realizar la actividad para evitar o eliminar los puntos de riesgos.

10.5 Acciones de fortalecimiento de los controles

Después de valorar los controles existentes, el riesgo residual permanece en zona moderada, alta o extrema, el proceso debe formular acciones de fortalecimiento orientadas a robustecer los controles vigentes o a crear nuevos controles que disminuyan la probabilidad o el impacto. El conjunto de estas acciones constituye el *Plan de Acción de Fortalecimiento de Riesgos de la Entidad.*

Este plan es distinto de un plan de contingencia: este último se enmarca en el Plan de Continuidad del Negocio y corresponde a un control correctivo, mientras que las acciones de fortalecimiento tienen un enfoque preventivo de mejora de los controles.

Cómo redactar las acciones de fortalecimiento

Cada acción de fortalecimiento debe ser concreta, verificable y dirigida a atacar la causa raíz del riesgo. Su redacción inicia con un verbo de acción (elaborar, implementar, documentar, automatizar, capacitar, actualizar) y precisa, como mínimo, los siguientes atributos:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Atributo	Descripción
Descripción de la acción	Qué se va a hacer para fortalecer o crear el control, redactada con un verbo de acción y de forma específica, asegurando el cómo y el fin de esta.
Producto o evidencia	Entregable que demuestra el cumplimiento de la acción (procedimiento, instructivo, registro, reporte, capacitación, etc.).
Fecha de inicio	Fecha a partir de la cual comienza la ejecución de la acción.
Fecha de finalización	Fecha máxima de cumplimiento, dentro del periodo de cobertura del Plan.

Ejemplo de redacción: *«Documentar e implementar un procedimiento de seguimiento a los términos de respuesta de las PQRSD, con alertas automáticas a cinco días del vencimiento». Evidencia: procedimiento publicado y reporte de alertas.*

Formulación, periodo de cobertura y cumplimiento

- Las acciones de fortalecimiento son formuladas por los procesos (primera línea), con el acompañamiento del GIT de Planeación.
- Se revisan por lo menos una vez al año, en el marco de la actualización de los mapas de riesgos.
- Su periodo de cobertura se extiende desde el 01 de enero hasta el 31 de diciembre de cada vigencia; no obstante, pueden cumplirse en cualquier momento dentro de dicho periodo.

Parametrización y seguimiento en la herramienta para la implementación del sistema de gestión dispuesto por la Entidad.

- El seguimiento a las acciones de fortalecimiento se realiza mediante la herramienta para la implementación del sistema de gestión dispuesto por la Entidad.
- El GIT de Planeación acompaña a los procesos y es el responsable de cargar las acciones de fortalecimiento en esta herramienta.
- Los procesos deben reportar cuatrimestralmente el avance y las evidencias del cumplimiento de sus acciones en esta herramienta.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- El GIT de Planeación, como segunda línea, realiza el monitoreo y la verificación del seguimiento reportado por los procesos.
- En el mismo informe cuatrimestral de seguimiento a los riesgos institucionales va incluido el monitoreo de estas acciones.

Monitoreo

Cada cuatro meses, los líderes de los procesos con el apoyo de su equipo de trabajo, deben realizar el monitoreo a la gestión de sus riesgos en la herramienta para la implementación del sistema de gestión de la entidad.

El monitoreo, que consiste en el seguimiento que se hace para determinar el estado del Sistema, corresponde a la primera línea, particularmente, a los líderes de proceso. En esa medida, los líderes, junto con sus equipos, son los responsables de generar los reportes sobre el estado de la gestión de los riesgos operativos, fiscales, y de los riesgos en el marco del SIGRIP.

El reporte del monitoreo realizado debe contener la información relacionada con:

Estado de aplicación del control: Descripción de la operación para cada control durante el periodo, de acuerdo con los cortes de monitoreo establecidos.

Evidencias de aplicación del control: Se deben adjuntar los soportes que evidencien la operación del control durante el periodo o citar la URL donde se encuentran ubicadas.

Avance en el Plan de Acción de Fortalecimiento de Riesgos de la Entidad: Se debe reportar el avance presentado en el desarrollo de las acciones formuladas por el proceso (si las hay) para crear nuevos controles o fortalecer los ya existentes, así como la evidencia que den cuenta de la gestión realizada.

Cuando las acciones del plan de manejo del riesgo hayan sido culminadas, el proceso debe hacer el análisis de las acciones implementadas para determinar si su implementación ha contribuido a la mitigación del riesgo y hacer la evaluación para establecer la nueva zona de riesgo residual en donde se ubicaría el riesgo luego de la aplicación de los nuevos controles.

Lo anterior se efectúa en la herramienta para la implementación del sistema de gestión dispuesto por la Entidad.

Materialización del Riesgo: Se debe reportar si en el periodo evaluado, el riesgo se materializó o no. En caso de que en el periodo evaluado se presente la materialización de un riesgo, se debe reportar la aplicación de los controles

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

correctivos definidos por el proceso con sus respectivas evidencias. Adicional a lo anterior, en caso de la materialización de un riesgo de integridad el proceso debe demostrar, la puesta en conocimiento ante las autoridades o entes de control que regulan la gestión de la Unidad (Fiscalía, Contraloría General de la República, Procuraduría General de la Nación, Control Interno Disciplinario, etc.)

Tras la materialización de un riesgo, el proceso debe registrar la información de lo ocurrido en el formato ***Base Histórica de Eventos – FO-SIG-043*** y realizar la revisión integral del riesgo y sus controles, con el fin de determinar cuál de ellos falló o no fue aplicado, causando la materialización del riesgo.

Finalmente debe definir acciones encaminadas a fortalecer los controles existentes o a crear nuevos controles buscando evitar que se vuelva a presentar una materialización.

Evaluación

A partir de la información registrada por los líderes de los procesos frente al monitoreo de sus riesgos en la herramienta para la implementación del sistema de gestión dispuesto por la Entidad, los procesos de la entidad, como primera línea, realizarán el reporte y seguimiento de la gestión integral del riesgo en las siguientes fechas:

SEGUIMIENTO	FECHA DE CORTE	FECHA DE REPORTE POR PARTE DE LA PRIMERA LINEA- PROCESOS
Primer Seguimiento	30 de abril Primer Cuatrimestre	Primeros cinco (05) días hábiles del mes de mayo
Segundo Seguimiento	31 de agosto Segundo Cuatrimestre	Primeros cinco (05) días hábiles del mes septiembre
Tercer Seguimiento	31 de diciembre Tercer Cuatrimestre	Primeros (10) días hábiles del mes enero de la siguiente vigencia.

Corresponde a la segunda línea en este caso el GIT de Planeación medir y analizar los resultados del monitoreo reportado por la primera línea, de forma que pueda llevar a cabo una evaluación objetiva respecto a la aplicación del control, los avances en el plan de tratamiento y el desarrollo de las acciones en caso de materialización de los riesgos. Este proceso se realiza mediante la herramienta para la implementación del sistema de gestión dispuesto por la Entidad.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

MONITOREO	FECHA DE CORTE	FECHA DE REPORTE POR PARTE DE LA SEGUNDA LINEA- GIT PLANEACIÓN
Primer Monitoreo	30 de abril Primer Cuatrimestre	Primeros diez (10) días hábiles del mes de mayo
Segundo Monitoreo	31 de agosto Segundo Cuatrimestre	Primeros diez 10) días hábiles del mes septiembre
Tercer Monitoreo	31 de diciembre Tercer Cuatrimestre	Primeros diez (15) días hábiles del mes enero

La evaluación implica, además, determinar el cumplimiento de los objetivos definidos para el SIGRIP y el estado de cada uno de sus elementos y herramientas.

Adicionalmente, el GIT de Planeación acompaña al proceso en la valoración y evaluación de los nuevos controles definidos por el proceso producto del desarrollo de su Plan de Tratamiento de Riesgos con el fin de establecer su nueva zona de riesgo residual cuando sea necesario.

En caso de materialización del riesgo, el Grupo Interno de Trabajo – Planeación debe revisar si el proceso reporto la aplicación de los controles correctivos definidos con el fin de restaurar el riesgo a los niveles predefinidos de operación. Adicionalmente, en caso de la materialización de un riesgo de integridad la debe verificar, que la situación se haya puesto en conocimiento de las autoridades o entes de control que regulan la gestión de la UPIT (Fiscalía, Contraloría General de la República, Procuraduría general de la Nación, Control Interno Disciplinario, etc.)

Tras la materialización de un riesgo identificado, el proceso donde se materializó el riesgo con el acompañamiento del Grupo Interno de Trabajo – Planeación debe velar por que el proceso registre la información de lo ocurrido en el formato ***Base Histórica de Eventos – FO-SIG-043***. Se debe realizar nuevamente la revisión y evaluación del riesgo y sus controles, así como la definición de acciones de fortalecimiento que busquen evitar que se vuelva a presentar una materialización. Esta acción se debe realizar en la herramienta para la implementación del sistema de gestión dispuesto por la Entidad.

- **Auditoría**

El Asesor Control Interno de acuerdo con los ciclos y alcance establecidos en el plan anual de auditoría, realizará la evaluación independiente de los riesgos identificados y gestionados en la Entidad.

Para el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP El Asesor de Control Interno como tercera línea debe realizar una evaluación independiente del Sistema para determinar su conformidad y eficacia, tanto del conjunto como de los controles individualmente vistos. La auditoría debe hacerse conforme a las

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

técnicas vigentes, al plan de auditoría de la entidad y desde un enfoque basado en riesgos.

- **Mejora**

Posterior a la emisión del informe emitido por el Asesor de Control Interno, los procesos con acompañamiento del Grupo Interno de Trabajo Planeación deben realizar los ajustes a sus riesgos y controles a los que haya lugar, estos cambios deben ser aprobados por el líder del proceso y la Coordinación del Grupo Interno de Trabajo Planeación con el fin de que los ajustes realizados sean incluidos en los mapas que serán objeto de revisión en el siguiente seguimiento. Se sugiere que con el acompañamiento del GIT de Planeación se realice un acta de reunión donde queden establecidos los cambios o verificaciones realizadas.

Una vez el proceso haya remitido el acta de reunión debidamente firmada al GIT de Planeación, se procederá con el ajuste y actualización en la herramienta para la implementación del sistema de gestión dispuesto por la Entidad. La anterior actividad la realizará la persona encargada de la administración del módulo de riesgos en la herramienta definida por la entidad.

Respecto del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, la mejora corresponde a la Alta Dirección o línea estratégica, quien lleva a cabo la revisión integral del Sistema. Este proceso de mejora debe ser continuo, y nutrirse de los reportes que se generan en el monitoreo, las evaluaciones y las auditorías.

En todo caso se deben implementar los planes de mejoramiento que se requieran, para atender a los hallazgos y no conformidades identificadas por la auditoría. También, deben tenerse en cuenta, desde el enfoque preventivo, las evaluaciones y los resultados del monitoreo.

11. Gestión de Riesgos Fiscales

Este capítulo tiene como finalidad orientar el análisis para identificar y gestionar los riesgos que puedan provocar un daño patrimonial al Estado, el cual en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado.

Como complemento para la identificación del riesgo fiscal es necesario tener en cuenta las siguientes consideraciones.

Para este ejercicio, se sugieren las siguientes preguntas orientadoras, descritas a continuación:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Sirve para Identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal?
Puntos de riesgo fiscal y circunstancias inmediatas	¿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-.
Circunstancias inmediatas	En un ejercicio autocritico, 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?

- **Identificación de áreas de impacto**

Dentro del contexto de riesgo fiscal, el área de impacto ***siempre*** corresponderá a una **consecuencia económica** sobre el patrimonio de la Entidad, a la cual se vería expuesta la UPIT en caso de materializarse el riesgo.

- **Identificación 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

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público
- Multas impuestas por hechos que no comportan gestión fiscal
- Existencia de actuación de cobro coactivo por parte de la entidad.
- Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.
- Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su "normal uso" (máquinas eléctricas, computadores, celulares, etc.). (Contraloría General de la República, 2023, p. 12).

12. Riesgos De Seguridad De La Información

En concordancia con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7 del DAFP, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos de la Política de Gobierno Digital, la gestión de los riesgos asociados a la seguridad de la información en la entidad se desarrolla bajo un enfoque integral de seguridad digital. Este enfoque reconoce que la protección de la información constituye un componente fundamental de la seguridad digital, la cual comprende además la protección de los servicios digitales, la infraestructura tecnológica, las redes, las aplicaciones y demás activos que soportan la operación institucional.

El objetivo de este capítulo es orientar la implementación del proceso de gestión de riesgos de seguridad de la información, con el propósito de fortalecer la confianza de las partes interesadas en el entorno digital institucional y contribuir a la protección de los activos de información y demás recursos tecnológicos que soportan el cumplimiento de la misión de la entidad.

En este contexto, el presente capítulo desarrolla los lineamientos para la identificación y valoración de activos de información, amenazas, vulnerabilidades y riesgos, así como para su análisis, evaluación, tratamiento, monitoreo, seguimiento y reporte, mediante la definición e implementación de controles orientados a preservar la confidencialidad, integridad y disponibilidad de la información institucional.

Para efectos de la gestión institucional del riesgo, los riesgos de seguridad de la información serán administrados como parte integral de la Matriz de Riesgos de Seguridad Digital de la entidad, permitiendo una visión unificada de los riesgos que puedan afectar la información, los activos tecnológicos, los servicios digitales y la continuidad de la operación institucional.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

A continuación, se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la Disponibilidad, Integridad y Confidencialidad de los activos de información contribuyendo de esta manera al cumplimiento de la misión y Visión de la UPIT.

Paso 1. Identificación y descripción de riesgos de seguridad de la información

a. Identificación de los activos de información:

En primer lugar, se deben identificar los activos de Información[5] mediante las actividades descritas en los "***Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional***" del MSPI, en ésta se presenta los lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación y clasificación de activos de información de cada entidad.

Se deben listar cada uno de los activos de información de la UPIT que corresponden al alcance del proyecto, luego, para cada activo se deben registrar los siguientes datos:

Proceso: Proceso de la Entidad al que pertenece el activo de información.

Identificador: Se sugiere que el identificador sea una concatenación del código de la dependencia según la Tabla de Retención Documental (TRD) + número consecutivo.

Tipo: Define el tipo de Activo de Información:

- **Información y datos de la entidad**: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros

- **Sistemas de información y aplicaciones de Software**: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.

[5] Identificación del activo de información (Ley 594 de 2000 - Ley 1712 de 2014- Decreto 103 de 2015 - Decreto 1080 de 2015 - ISO 27001)

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- **Dispositivos de Tecnologías de información- Hardware**: Equipos de cómputo que por su criticidad son considerados activos de información, no sólo activos fijos.
- **Soporte para almacenamiento de información**: Equipo para almacenamiento de información como USB, Discos Duros, CDs, SAN, NAS.
- **Servicios**: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- **Instalaciones**
- **Redes**

Oficina: Área, dependencia o proceso que está identificando el activo de información.

Serie documental: Serie documental del área, dependencia o proceso que se encuentra identificando el Activo.

Subserie documental: Subserie documental del área, dependencia o proceso que se encuentra identificando el Activo.

Nombre: Nombre completo del activo de información.

Descripción: Descripción resumida de manera clara para identificar el activo de información.

Nombre del responsable de la producción de la información (Propietario del activo): Nombre del área, dependencia, proceso responsable de producir el activo de información

Fecha de generación de la información: Fecha en la que el activo de información fue incluido en el inventario – TRD.

Nombre del responsable de la información (Custodio del activo): Corresponde al nombre del área, proceso o dependencia encargada en la Entidad de la custodia o control de la información o implementación de controles de protección.

Fecha de ingreso del activo al archivo: Fecha en la que el activo ingresa al archivo de gestión.

Soporte de registro: De acuerdo con el Decreto 2609 de 2012:

- **Físico** (análogo)

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- **Digital** (electrónico) Este campo se diligencia si el Tipo de activo es "Información"
- **N/A:** Para el resto de los tipos de activos se debe seleccionar N/A.

Medio de conservación: De acuerdo con el Decreto 2609 de 2012 Archivo Institucional Es la instancia administrativa de custodiar, organizar y proteger.

Formato: Identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: Hoja de cálculo, imagen, audio, video, documento de texto, etc.

Idioma: Establece el idioma, lengua o dialecto en que se encuentra la información.

b. Clasificación Del Activo De Información (ISO 27001)

A continuación, se realiza la Clasificación de Activos de Información de acuerdo con los siguientes criterios de clasificación:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad.**
- **Criticidad del activo**

Donde 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 como se muestra a continuación:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	**ALTA (A)**	**ALTA (1)**
INFORMACIÓN PUBLICA CLASIFICADA	**MEDIA (M)**	**MEDIA (2)**
INFORMACIÓN PÚBLICA	**BAJA (B)**	**BAJA (3)**
NO CLASIFICADA	**NO CLASIFICADA**	**NO CLASIFICADA**

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

El nivel de clasificación del activo corresponderá con el resultado de la sumatoria de la tabla de criterios de clasificación, que se muestra en la siguiente tabla.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Este resultado corresponde con el nivel de Criticidad del activo.

- **Es Infraestructura Critica cibernética Nacional**: Se define si el activo corresponde con los criterios de Infraestructura Critica cibernética descritos en los "lineamiento para la identificación de las infraestructuras críticas cibernéticas" del MSPI.
- **Información publicada**: Se define si el activo está publicado en la intranet, en internet o no está publicado.
  - **Publicada**: Si la información es publica y se puede consultar en un sitio web (interno o externo) o un sistema de información del Estado.
  - **Publicada** (Interno - Intranet)
  - **Publicada** (Externo - Internet)
  - **No Publicada**: Si la información se encuentra en la Entidad, pero no se encuentra en un sistema de información o sitio web.
- **Lugar de consulta o ubicación**: Indica la URL, sitio web o sistema de información donde puede ser consultada la información si esta se encuentra pública, el lugar de consulta si no está publicada o ubicación física.

Clasificación de Activos

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)						
Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	Es Infraestructura Crítica cibernética	Información Publicada	Lugar de consulta o ubicación

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

c. Índice De Información Clasificada Y Reservada

El Índice de Información Clasificada y Reservada es el instrumento mediante el cual la entidad identifica, organiza y registra la información pública que, de conformidad con la Constitución, la Ley 1712 de 2014 y demás disposiciones aplicables, posee restricciones de acceso por razones de protección de derechos fundamentales, seguridad, defensa, reserva legal o interés público. Este índice permite conocer qué información tiene carácter clasificado o reservado, la norma que sustenta dicha restricción, el responsable de su custodia y el período durante el cual se mantiene la limitación de acceso, garantizando un adecuado equilibrio entre los principios de transparencia, acceso a la información pública y protección de la información sensible de la entidad.

El Índice de Información Clasificada y Reservada constituye un insumo fundamental para la gestión de la seguridad de la información, al facilitar la identificación de los activos de información que requieren medidas especiales de protección para preservar su confidencialidad y garantizar el cumplimiento de las disposiciones legales aplicables.

Para efectos de la matriz se registra mediante los siguientes campos de información:

- **Objeto legítimo de la excepción**: La identificación de la excepción que, dentro de las previstas en los artículos 18 y 19 de la Ley 1712 de 2014, cobija la calificación de información reservada o clasificada. Si la respuesta es **NO** se debe marcar no aplica (N/A) en los demás campos sobre el índice de información clasificada y reservada.
- **Fundamento constitucional o legal**: Indica el fundamento constitucional o legal que justifica la clasificación o la reserva, señalando expresamente la norma, articulo, inciso o párrafo que la ampara.
- **Fundamento jurídico de la excepción**: Indica la norma jurídica que sirve como fundamento jurídico para la clasificación o reserva de la información.
- **Excepción total o parcial**: Según sea integral o parcial la calificación, las partes o secciones clasificadas o reservadas. Indicar si la totalidad del documento es clasificado o reservado o si solo una parte corresponde a esta calificación
- **Fecha de clasificación (DD/MM/AAAA)**: Fecha en que se calificó la información como reservada o clasificada.
- **Tiempo de clasificación**: Tiempo que cobija la clasificación o reserva. La clasificación es ilimitada en años, la reserva solo puede durar como máximo por 15 años desde la creación del documento.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Índice de Información Clasificada y Reservada

INDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA (DECRETO 103 DE 2015)					
Objeto legítimo de la excepción	**Fundamento constitucional o legal**	**Fundamento jurídico de la excepción**	**Excepción total o parcial**	**Fecha de clasificación (DD/MM/AAAA)**	**Tiempo de clasificación**

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

d. Datos Personales (Ley 1581 De 2012)

El siguiente bloque corresponde con los activos de información que contienen datos personales:

- **¿Contiene datos personales?:** ¿El activo de información contiene datos personales? SI - NO
- **¿Contiene datos personales de niños, niñas o adolescentes?:** Son los datos personales de los niños, niñas y adolescentes, cuyo tratamiento está prohibido, salvo que se trate de datos de naturaleza pública. Ej. Registro civil.
- **Tipos de datos personales**: Si cuenta con datos personales seleccione el tipo, en caso contrario seleccione N/A:
  - **Dato personal público**: Toda información personal que es de conocimiento libre y abierto para el público en general. Ejemplo: Número de identificación apellidos.
  - **Dato personal privado**: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general. Ejemplo: Dirección de residencia y Nº teléfono.
  - **Dato semiprivado**: Es semiprivado el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector y grupo de personas. Ejemplo: Fecha y lugar de nacimiento

Finalidad de la recolección de los datos personales: La finalidad de la recolección justifica por la cual el dato es capturado, almacenado y mantenido en la Entidad

Existe la autorización para el tratamiento de los datos personales: Seleccionar si se cuenta o no con la autorización de la recolección y tratamiento.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Datos Personales

DATOS PERSONALES (LEY 1581 DE 2012)				
¿Contiene datos personales?	**¿Contiene datos personales de niños, niñas o adolescentes?**	**Tipos de datos personales**	**Finalidad de la recolección de los datos personales**	**Existe la autorización para el tratamiento de los datos personales**

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

e. Aprobación de la Identificación, Clasificación y valoración de Activos

"Posterior a la identificación, clasificación y valoración de los activos de información compilados en la Matriz de Activos de Información por los líderes de los procesos, se debe enviar la matriz para su consolidación y validación por parte de la Oficina Asesora Jurídica para finalmente ser presentada ante el Comité Institucional de Gestión y Desempeño."

Finalmente se realiza el etiquetado de la información para que los usuarios puedan establecer el nivel de confidencialidad de cada documento.

El resultado de esta actividad es la Matriz del Inventario de Activos de Información que es el insumo principal para la Gestión de Riesgos de Seguridad de la Información proceso que se encuentra descrito en la Guía "*Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas*".

Se debe establecer según el nivel de criticidad a cuáles activos se les realizará el correspondiente análisis de riesgos.

A continuación, se desarrolla un ejemplo práctico:

i) Listado y registro de activos, asociando macroproceso, proceso, identificador, tipo, serie y subserie documental:

Proceso	Identificador	Tipo	Oficina	Serie documental	Subserie documental
Gestión Financiera	GF001	Software	Financiera	001	00001
Gestión Financiera	GF001	Software	Financiera	001	00001

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

ii) Datos sobre el activo de información, sus responsables, soportes de almacenamiento de información, servicios, soporte registro, medio conservación, idioma.

Nombre	Descripción	Nombre del responsable de la producción de la información (Propietario del activo)	Fecha de generación de la información	Nombre del responsable de la información (Custodio del activo)
Software de gestión de nómina (Pagosnet)	Software de gestión de nomina	Director TI	12/03/2025	Analista nomina
Informe pagos de nómina periodo: ene-2025 a marzo-2025	Informe de los pagos de nómina realizados den el periodo: ene-2025 a marzo-2025	Director Financiero	12/03/2025	Analista nomina
Fecha de ingreso del activo al archivo	**Soporte de registro**	**Medio de conservación**	**Formato**	**Idioma**
22/11/2000	Digital	Sistemas de Información corporativos	Software de gestión de nomina	Español
22/11/2000	Digital	Sistemas de Información corporativos	Software de gestión de nomina	Español

iii) Clasificación de los activos, de acuerdo con el análisis sobre el nivel de criticidad para cada uno:

Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	¿Es Infraestructura Critica Cibernética?	Información publicada	Lugar de consulta o ubicación
Clasificada / Uso Interno = Medio	Alto	Alto	ALTA	No	Publicada (Interno - Intranet)	Intranet
Clasificada / Uso Interno = Medio	Alto	Alto	ALTA	No	Publicada (Interno - Intranet)	Sharepoint

Objeto legítimo de la excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción total o parcial	Fecha de clasificación (DD/MM/AAAA)	Tiempo de clasificación
N/A	N/A	N/A	N/A	N/A	N/A

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Si	artículo 18 de la ley 1712 de 2014	artículo 18 de la ley 1712 de 2014	Reserva parcial	15/03/2025	15 años

¿Contiene datos personales?	¿Contiene datos personales de niños, niñas o adolescentes?	Tipos de datos personales	Finalidad de la recolección de los datos personales	Existe la autorización para el tratamiento de los datos personales
N/A	N/A	N/A	N/A	N/A
Si	No	Dato semiprivado	Realizar el pago de nomina	Si

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

f. Proceso De Gestión De Riesgos De Seguridad De La Información

Una vez realizada la identificación y valoración de los activos de información asociados al entorno digital de la entidad, se procederá a la consolidación de la información en la Matriz de Riesgos de Seguridad Digital, la cual constituye el instrumento mediante el cual se registran, analizan, evalúan y gestionan los riesgos identificados.

Para este propósito, la Matriz de Riesgos de Seguridad Digital de la entidad utiliza la clasificación de pérdida de confidencialidad, integridad y disponibilidad establecida por el Modelo de Seguridad y Privacidad de la Información (MSPI) para los riesgos asociados a los activos de información, sin perjuicio de que los impactos identificados puedan extenderse a los servicios digitales, la infraestructura tecnológica y la continuidad operativa. De esta manera, la entidad adopta una visión integral de la gestión del riesgo, articulando la protección de la información con la protección del entorno digital que soporta el cumplimiento de su misión institucional.

La cual inicia con el registro de los siguientes campos:

Matriz de Riesgos de Seguridad de la Información			
Proceso	Referencia	Activo de Información	Tipo de Activo

Para el diligenciamiento de la anterior matriz se describe cada aspecto:

Proceso: Proceso al cual se encuentra asignado el activo de información.

Referencia: Es el número del ítem del activo de información.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Activo de Información: Es el nombre del activo de información.

Tipo de Activo: Corresponde a una de las siguientes categorías:

- ✓ Información
- ✓ Software
- ✓ Hardware
- ✓ Servicios
- ✓ Intangibles
- ✓ Infraestructura crítica cibernética nacional
- ✓ Recursos humanos
- ✓ Instalaciones y Otros Servicios

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.

Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la siguiente tabla se definen los elementos necesarios:

i. Amenazas y Vulnerabilidades

Matriz de Riesgos de Seguridad Digital	
Amenazas (Causa Inmediata)	Vulnerabilidades (Causa Raíz)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).

Las amenazas pueden ser Deliberadas(D), fortuitas (F) o Ambientales (A)

Tabla de Amenazas Comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Tipo	Amenaza	Origen
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas Técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

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

Tabla de Vulnerabilidades Comunes:

Tipo	Amenaza
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

ii. Descripción del riesgo

En este paso se identifican:

Matriz de Riesgos de Seguridad de la Información		
Tipo de Riesgo	Descripción del Riesgo	Clasificación Riesgo

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

- **Tipo de Riesgo**: Este campo solo admite uno de estos 3 valores:
  - Pérdida de Disponibilidad

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Pérdida de Integridad
- Pérdida de Confidencialidad

- **Descripción del Riesgo**: En este campo se describe la situación específica que da como resultado el correspondiente riesgo.

"*Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita*."

Si requiere información adicional remitirse al punto *Descripción del riesgo* de este mismo documento.

Clasificación del Riesgo: Este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad.

Paso 2 Análisis de Riesgo Inherente

A partir de este paso metodológico se incorporan la tablas y matrices establecidas en el numerales anteriores que desarrolla los lineamientos para los riesgos generales de la gestión.

iii. Determinar la probabilidad

En esta actividad se debe realizar el análisis de probabilidad de la materialización de estos riesgos.

Matriz de Riesgos de Seguridad de la Información		
Frecuencia	% Probabilidad Inherente	Probabilidad Inherente

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

- **Frecuencia**: Este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.
- **% Probabilidad Inherente**: Este campo corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa de acuerdo con la tabla *Criterios para definir el nivel de probabilidad* del numeral Determinación de la probabilidad inherente.
- **Probabilidad inherente**: Este campo corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa de acuerdo con la tabla *Criterios para definir el nivel de probabilidad* del numeral Determinación de la probabilidad inherente.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Probabilidad	Frecuencia de la Actividad	% Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces al año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 501 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

iv. Determinación del Impacto

En esta actividad se continua con la metodología general de gestión del riesgo que se describe a continuación: análisis del impacto de la materialización de estos riesgos.

Impacto	
% Impacto Inherente	Impacto Inherente

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

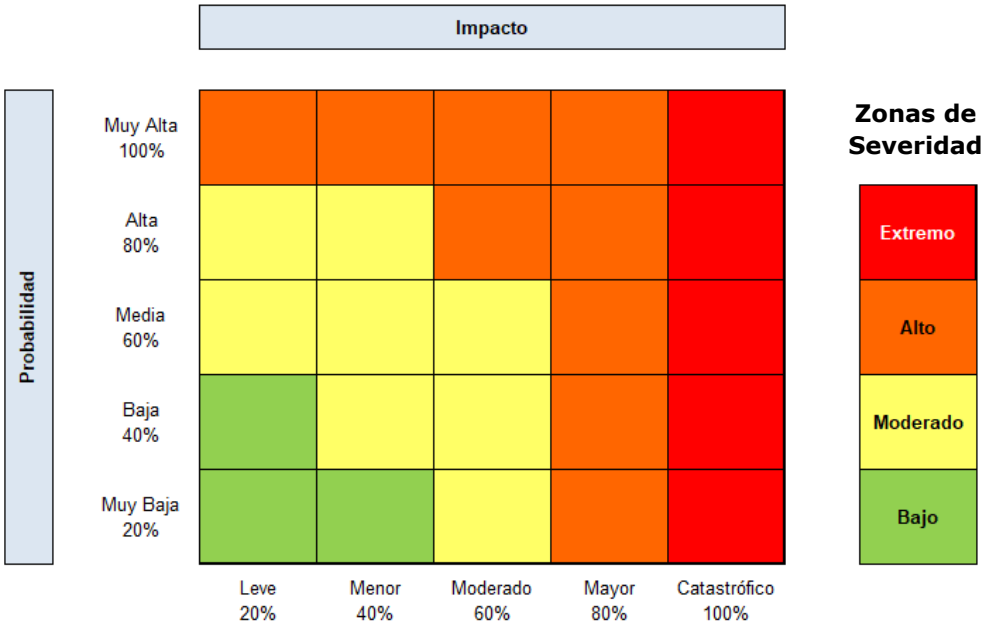
- **% Impacto Inherente**: Este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa de acuerdo con la tabla *Criterios para definir el nivel de probabilidad* del numeral Determinación del impacto inherente.
- **Impacto Inherente**: Este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa de acuerdo con la tabla *Criterios para definir el nivel de probabilidad* del numeral Determinación del impacto inherente.

Impacto	Afectación Económica	Reputacional	% Probabilidad
Leve	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.	20%

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Menor	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y/o de proveedores.	40%
Moderado	Mas de 50 y hasta 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	60%
Mayor	Mas de 100 y hasta 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	80%
Catastrófico	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país	100%

Zona de riesgo inherente: En este campo se determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto, tal como se muestra en la tabla matriz de calor para análisis de severidad del numeral Análisis de Severidad.



La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Paso 3: Diseño y Análisis de Controles

v. Estructura para la Descripción del Control

En esta actividad se seleccionan los controles que se establecerán para mitigar los riesgos.

No. Control	Control Anexo A	Descripción del Control

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

- **No. Control**: Este campo es un consecutivo de los controles a establecer.
- **Control Anexo A**: Este campo corresponde al control seleccionado del Anexo A de la norma 27001:2022.
- ***NOTA**: Se podrán crear controles adicionales a los listados en el anexo A de la norma ISO 27001:2022 de acuerdo a las necesidades de los procesos que identifican y gestionan los riesgos.*
- **Descripción del Control**: Este campo corresponde a una descripción de la forma en la cual el control seleccionado será implementado en la entidad.

***NOTA**: Se recomienda se establezca para cada control técnico el correspondiente control administrativo, de tal manera que estos se complementen y potencialicen.*

vi. Valoración de Controles

- **Afectación:** En esta actividad se establece la afectación que tendrá la implementación del control sobre la Probabilidad o el Impacto del riesgo.

AFECTACIÓN	
Probabilidad	Impacto

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

- **Probabilidad**: En este campo se especifica si el control pretende modificar la probabilidad de ocurrencia de riesgo.
- **Impacto**: En este campo se especifica si el control pretende modificar el impacto de ocurrencia de riesgo.

vii. Atributos

En esta actividad se establecen los Atributos de la implementación del control, donde se consideran atributos de eficiencia y los de formalización del control, de acuerdo con las siguientes tablas:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Análisis atributos de eficiencia

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación *Nota: En implementación no se tienen controles semiautomáticos	Automático	25%
	Manual	15%

Análisis atributos formalización del control

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios,

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Características de Eficiencia		Descripción
		confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Atributos

ATRIBUTOS							
Tipo	**%**	**Implementación**	**%**	**Calificación del control**	**Documentación**	**Frecuencia**	**Evidencia**

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

Paso 4: Valoración de Riesgo Residual

g. Valoración Del Riesgo Residual

En esta etapa se revisa la efectividad de los controles, aplicándolos de acuerdo con la tabla "**Aplicación de controles para establecer el riesgo residual**" que hace parte del numeral de Aplicación de controles en la matriz de severidad de manera que al final se pueda determinar el riesgo residual.

Valoración del Riesgo Residual

VALORACIÓN DEL RIESGO RESIDUAL				
Probabilidad Residual	**% de Probabilidad Residual**	**Impacto Residual**	**% Impacto Residual**	**Zona de Riesgo Final**

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

h. Plan de implementación de controles

En esta actividad se establece un plan para implementar los controles y poder realizar el correspondiente seguimiento:

PLAN DE IMPLEMENTACIÓN DE CONTROLES					
Tratamiento	**Plan de Acción**	**Responsable**	**Fecha de Implementación**	**Seguimiento**	**Estado**

- **Tratamiento**: En este campo se especifica el tipo de tratamiento que se realizará entre 4 opciones disponibles:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

  - **Reducir**: Implementar controles para reducir la probabilidad o el impacto
  - **Compartir**: Compartir las consecuencias de la materialización del riesgo, por ejemplo, a través de la adquisición de una ciber póliza
  - **Aceptar**: Cuando el nivel del riesgo está por debajo del apetito establecido por la alta dirección.
  - **Evitar**: Cuando se decide eliminar el activo que es fuente del riesgo: por ejemplo, dar de baja un servidor.
- **Plan de Acción**: En este campo se especifica la identificación del Plan de acción con el cual se realizará la implementación de dicho control.
- **Responsable**: En este campo se especifica el cargo de quien implementa el control.
- **Fecha de Implementación**: En este campo se especifica la Fecha máxima de implementación del control.
- **Seguimiento**: En este campo se especifica la periodicidad del seguimiento a la implementación del control.
- **Estado**: En este campo se especifica el estado de la implementación del control.

13.Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP

El SIGRIP nace como una herramienta que busca ***prevenir***, ***detectar*** y ***corregir*** los eventos que amenazan el ejercicio íntegro del **servicio público** (riesgos asociados a Corrupción) o la **integridad de las instituciones del Estado** (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción).

Amenazas para la integridad pública

Hay varias amenazas que pueden incidir en diferentes puntos de los procesos de la Entidad, que terminan afectando su capacidad para alcanzar los objetivos planteados, en particular, asegurar el cumplimiento de la ley. A continuación, se describen cinco amenazas para la integridad del servicio público que pueden afectar a la UPIT.

Soborno

El Soborno puede ser entendido como ***"ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la***

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar [...]"[6].

El soborno opera en dos niveles: Soborno Entrante y Saliente. Se entiende como Entrante el soborno al servidor de la Entidad, y como Saliente el soborno por parte de servidores a otros en nombre de la Entidad.

El Código Penal Colombiano tipifica el cohecho propio, el cohecho impropio, el cohecho por dar u ofrecer, todos estos delitos contra la administración pública, que son formas de soborno. Solamente entre particulares tipifica de forma general el soborno.

Fraude

El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con **culpa o dolo** para beneficio personal o de terceros[7]. Este puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima.

El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.

Inadecuada gestión del conflicto de intereses:

Un conflicto de intereses[8] surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando ***el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.***

Si bien la sola existencia del conflicto de intereses no implica una conducta reprochable, sí existen una serie de comportamientos definidos por códigos de conducta sobre la declaración y gestión del conflicto de intereses. La legislación

---

[6] Definición de soborno según la norma ISO 37001:2025 - Sistemas de gestión antisoborno. Requisitos con orientación para su uso.
[7] Concepto construido a partir de los términos y definiciones utilizados por la Organización Internacional de Normalización (ISO, por sus siglas en inglés).
[8] Concepto construido a partir de lo establecido en el artículo 44 de la Ley 1952 de 2019, *"Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario"*

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

nacional estima que quien tenga un interés particular en un asunto público está impedido para tomar la decisión.

Corrupción

La Corrupción es *todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero*. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral"[9].

Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP

La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la **capacidad del Estado** para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento.

14. Sistema de Gestión del Riesgo

Teniendo en cuenta las diferentes amenazas para la integridad pública definidas en el punto anterior, es necesario que, desde un enfoque basado en riesgos, se gestionen los eventos que pueden ocurrir dentro de la Unidad. Esto implica que en la Entidad se deben ***identificar, analizar y valorar los riesgos, partiendo de la existencia de eventos que pueden convertirse en factores de riesgo.***

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, busca articular la Política para la Gestión Integral de Riesgos, mediante la cual se

[9] Según el artículo 2.1.4.3.1.3 del Decreto 1081 de 2015.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

gestionan los Riesgos Generales de la Gestión, Fiscales y de Seguridad de la Información, con los demás elementos que son necesarios para gestionar los riesgos para la integridad pública, los cuales se describen a continuación.

Al final, un riesgo de gestión, un riesgo fiscal o un riesgo de seguridad de la información puede tener como causa el soborno, el fraude, un conflicto de intereses gestionado inadecuadamente o la corrupción. Además, puede también favorecer el lavado de activos, la financiación del terrorismo o la financiación de la proliferación de armas de destrucción masiva. Por esta razón, en el presente documento se abordan los riesgos para la integridad pública de forma integral y en estrecha articulación con la gestión institucional del riesgo.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP contempla que en la entidad se adopte una serie de instrumentos de gestión del riesgo, que actúe con diligencia en el conocimiento de sus contrapartes y que integre en su operación una función de cumplimiento, todo esto además de la identificación y valoración de los riesgos según la metodología definida en la Política para la Gestión Integral de Riesgos que adopte. El objetivo es que todos estos elementos interactúen para asegurar que la gestión pública se realice de forma íntegra, es decir, con el pleno cumplimiento de la ley en toda la gestión institucional.

El SIGRIP, además, permite dar cumplimiento a los lineamientos establecidos para la gestión de riesgos en los Programas de Transparencia y Ética Pública, según lo dispuesto por la Secretaría de Transparencia de la Presidencia de la República. En la medida que se implemente plenamente el Sistema, la entidad estará acreditando la gestión de riesgos para la integridad pública, de riesgos LA/FT/FP, canales de denuncia y debida diligencia.

En consecuencia, el presente Manual, la Política para la Gestión Integral de Riesgos y el mapa de riesgos para la integridad pública —incluido el mapa de riesgos de corrupción— hacen parte integral del Programa de Transparencia y Ética Pública (PTEP) de la UPIT y se articulan con sus demás componentes; su seguimiento se refleja en los informes del PTEP y en el seguimiento al MIPG de la Entidad.

14.1 Operación del SIGRIP

Como se comentó previamente, el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP es un conjunto de elementos que operan e interactúan entre sí.

El principal elemento del Sistema es la Política para la Gestión Integral de Riesgos, la cual se encuentra formulada y hace parte del presente documento; junto con su respectivo mapa de riesgos.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Esta política define los mecanismos mediante los cuales se identificarán y valorarán los diferentes riesgos a los que está expuesta la organización, incluidos los riesgos para la integridad pública. Sin embargo, esta Política no es suficiente para gestionar completamente los riesgos asociados a soborno, fraude, inadecuada gestión del conflicto de intereses, Corrupción, LA/FT/FP. Entonces, con el propósito de lograr una gestión integral, es que surgen los otros tres elementos del SIGRIP:

- La debida diligencia en el conocimiento de las contrapartes
- La función de cumplimiento
- Las herramientas de gestión del riesgo.

La estructura del SIGRIP se observa en la figura a continuación:

Sistema de Gestión de Riesgos para la Integridad Pública



Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

De acuerdo con la anterior estructura, se procede a describir las particularidades propias del SIGRIP que deben incluirse en la Política para la Gestión Integral de Riesgos, así como cada uno de los elementos adicionales con que debe contar cada entidad, y que en su conjunto derivan en un sistema integral de gestión del riesgo.

14.2 Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos

En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, las entidades deberán identificar y valorar los riesgos que pueden impactar el ejercicio íntegro de la función pública, incluidos los riesgos de LA/FT/FP.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Sin embargo, bajo una perspectiva de integralidad, ***los riesgos para la integridad pública deben ser gestionados en conjunto con los riesgos generales de gestión, la gestión preventiva del riesgo fiscal y los riesgos de seguridad de la información como se expusieron al inicio del documento***.

La existencia de una misma política para gestionar todos los riesgos implica que se debe aplicar, de forma general, una misma metodología. Es decir, para identificar y valorar los riesgos para la integridad pública se podrá aplicar la propuesta metodológica que se ha definido en el numeral *de Riesgos Generales de la Gestión Institucional* del presente manual.

Respecto de la "Identificación de los puntos de riesgo"

Respecto del riesgo de Corrupción ahora en adelante Riesgo de Integridad Pública y sus manifestaciones específicas como soborno, fraude e inadecuada gestión del conflicto de intereses, los puntos de riesgos pueden ser cualquier actividad dentro del flujo de proceso y no solo las operaciones.

Respecto de la "Identificación de áreas de impacto"

En el marco de la gestión de los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber **consecuencias legales** y de **contagio**.

La **consecuencia legal** corresponde al incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños. Así pues, el impacto legal surge desde el momento en que una contraparte es vinculada a procesos judiciales o administrativos sancionatorios o que busquen declarar un incumplimiento.

El **contagio** corresponde a la posibilidad de que la entidad pueda sufrir una afectación económica, reputacional o legal a causa de la acción propia de una entidad o de un individuo relacionado. El contagio se expresa cuando a partes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar a la entidad.

En la medida que la gestión del riesgo de ***LA/FT/FP*** está centrada en prevenir la utilización de la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas, aun cuando no haya consecuencias, toda operación sospechosa, incluso la intentada, debe ser objeto de reporte, al margen de la materialización del delito de lavado de activos.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Toda la gestión del riesgo tiene como principales objetivos la identificación, medición, control y el monitoreo, con el propósito de prevenir, detectar y corregir. En ningún caso podrá derivar en juicios de responsabilidad o en la aplicación de sanciones.

Respecto de la "Identificación de factores de riesgo"

Como factores del riesgo LA/FT/FP se tiene a las **contrapartes**, los **productos**, los **canales** y las **jurisdicciones**, aspectos mínimos a contemplar en cualquier análisis, los cuales en conjunto conforman el concepto de ***"transacción"*** **u** ***"operación"***, en el entendido que una transacción, en todos los casos, será realizada por un cliente o usuario, que accedió o entregó un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica. Estos factores deben permitirle a la entidad mayor efectividad en el conocimiento de las contrapartes, el diseño y aplicación de señales de alerta, la identificación de operaciones inusuales y la determinación y el reporte de operaciones sospechosas.

Surge, entonces, la necesidad de segmentación de los factores de riesgo, a partir de la cual, se profundiza tanto en el conocimiento de las contrapartes, así como de los factores de riesgo con los que tienen relación

El objetivo y los beneficios de la segmentación de los factores de riesgo se encuentran en la identificación de grupos con características y comportamientos similares, en los que se garantiza la homogeneidad al interior de los segmentos y la heterogeneidad entre los mismos, de acuerdo con el análisis técnico de variables de información.

Al garantizar las características de homogeneidad y heterogeneidad, cada uno de los segmentos genera implícitamente los parámetros normales de comportamiento transaccional de los miembros de cada grupo, lo que se entiende como los límites de operación de cada persona o comúnmente denominadas como las **señales de alerta** que se encargan de la identificación de las operaciones que salen de la normalidad identificada y que pueden ser catalogadas como operaciones inusuales objeto de estudio por parte de la función de cumplimiento, con el fin de efectuar los reportes oportunos a las autoridades competentes.

En este sentido, se hace obligatorio mantener los documentos y registros de las contrapartes y sus operaciones por el término dispuesto en el artículo 12 de la Ley 2195 de 2022; y asignar los recursos técnicos, tecnológicos y de talento humano para poder llevar a cabo la gestión de estos riesgos.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Respecto de la "Descripción del riesgo"

La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en el numeral en la Descripción del riesgo de gestión del presente documento.

Teniendo en cuenta las amenazas descritas en el numeral de 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 desplegados en la tabla a continuación:

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 persona actúe o se abstenga de actuar […]".	
	Conflicto de Intereses	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para	

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

		obtener un beneficio propio o para un tercero	

Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

En el caso particular del riesgo LA/FT/FP, debe hacerse referencia particularmente a las actividades del flujo de procesos en que existe la vulnerabilidad o exposición al riesgo, como se explica en la tabla a continuación.

Impacto	Causa Inmediata	Causa Raíz
Económico, Reputacional, Legal, Operativo o de Contagio	Usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva	Descripción de la Operación o Transacción

Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

Para el análisis del riesgo inherente, el diseño y análisis de controles se debe tener en cuenta los lineamientos definidos al inicio de este documento. Sin embargo, además de los controles definidos en el mapa de riesgos, la entidad debe asegurar que las herramientas del SIGRIP funcionen como controles transversales. Estos controles deben integrarse al Programa de Transparencia y Ética Pública y a la Política para la Gestión Integral de Riesgos definidas en este Manual.

Control transversal	Propósito
Manual de debida diligencia	Definir cómo se identifica, verifica, evalúa y monitorea a las contrapartes antes y durante la relación.
Política ALA/CFT/CFP	Prevenir el uso de la entidad para lavado de activos, financiación del terrorismo o proliferación de armas de destrucción masiva.
Política antisoborno	Prohibir y prevenir la solicitud, aceptación, ofrecimiento o entrega de ventajas indebidas.
Política antifraude	Prevenir manipulación de información, ocultamientos, falsedades o aprovechamiento indebido de recursos.
Procedimiento de conflictos de intereses	Definir cómo se declaran, tramitan, gestionan y controlan los conflictos de intereses.
Procedimiento de operaciones inusuales o sospechosas	Establecer señales de alerta, análisis, escalamiento y reporte a la función de cumplimiento y autoridades competentes.
Canal de denuncias y buzón ético	Recibir, evaluar, tramitar y cerrar denuncias o inquietudes asociadas a corrupción o conductas contrarias a la integridad.

Respecto de la "Valoración del riesgo residual"

Para la valoración del riesgo residual, se debe tener en cuenta el capítulo de Valoración de controles y Aplicación de controles en la matriz de severidad.

El riesgo residual corresponde al nivel de riesgo que permanece después de aplicar la efectividad de los controles. Para los riesgos del SIGRIP, esta valoración debe permitir determinar si el riesgo se mantiene dentro del nivel aceptado por la UPIT o si requiere acciones adicionales de tratamiento.

1. Verificar que cada control esté asociado a una causa raíz o factor de riesgo identificado.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

2. Evaluar la tipología y solidez del control: preventivo, detectivo, correctivo, manual o automático, documentado, con evidencia y responsable claro.
3. Aplicar la metodología institucional para ajustar la probabilidad y/o impacto según los controles existentes.
4. Determinar la nueva zona de riesgo residual en la matriz de severidad.
5. Comparar el resultado con el apetito, tolerancia y capacidad de riesgo definidos por la entidad.
6. Definir tratamiento cuando el riesgo residual sea superior al nivel aceptado.

Opciones de tratamiento

Opción	Aplicación práctica en SIGRIP
Aceptar	Cuando el riesgo residual se encuentra dentro del nivel aceptado y existen controles suficientes y documentados.
Reducir o mitigar	Cuando se requieren controles adicionales, ajustes al procedimiento, mayor supervisión, automatización, capacitación o debida diligencia reforzada.
Transferir o compartir	Cuando se requiere asegurar garantías, pólizas, cláusulas contractuales, interventorías, supervisiones especializadas u otras medidas permitidas.
Evitar	Cuando la exposición es no aceptable y la entidad debe abstenerse de iniciar, continuar o aprobar una relación, operación o actividad, conforme al marco legal aplicable.

Focos de riesgo para la integridad propios de la UPIT

Atendiendo el objeto misional de la UPIT de planear el desarrollo de la infraestructura de transporte de manera integral, indicativa, permanente y coordinada con los agentes del sector transporte, para promover la competitividad, conectividad, movilidad y desarrollo en el territorio nacional en materia de infraestructura de transporte, así como consolidar y divulgar la información requerida para la formulación de política en materia de infraestructura de transporte. la identificación de riesgos para la integridad debe considerar de manera prioritaria los siguientes focos de exposición:

- **Planeación y priorización de inversiones:** posible manipulación de estudios, modelos o criterios técnicos para favorecer determinados proyectos, corredores o agentes del sector.
- **Gestión de información:** uso indebido, alteración u ocultamiento de la información que la Unidad consolida y divulga para la formulación de política, o aprovechamiento de información privilegiada.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- **Contratación:** direccionamiento de estudios y consultorías, sobreestimación de necesidades, fraccionamiento o conflictos de interés en la estructuración y supervisión contractual.
- **Relacionamiento con agentes del sector:** Por intereses particulares en las entidades del sector, sector académico, agremiaciones y entidades territoriales.
- **Talento humano:** conflictos de interés no declarados, tráfico de influencias y vinculación o contratación sin verificación de inhabilidades e incompatibilidades.

Debida diligencia en el conocimiento de las contrapartes

La debida diligencia es el conjunto de actividades mediante las cuales la UPIT conoce a sus contrapartes (personas naturales o jurídicas con las que se relaciona) antes de iniciar la relación y durante toda su vigencia, con el fin de prevenir el uso de la Entidad para conductas contrarias a la integridad pública o para LA/FT/FP. Comprende, como mínimo:

- Identificación y verificación de la contraparte y, cuando aplique, de su beneficiario final.
- Consulta en listas restrictivas y fuentes de información públicas y vinculantes para Colombia.
- Evaluación del riesgo de la contraparte según los factores de riesgo (contrapartes, productos, canales y jurisdicciones) y su segmentación.
- Monitoreo continuo de la relación y actualización de la información, con debida diligencia reforzada para contrapartes de mayor riesgo.

Flujo de reporte de operaciones inusuales y sospechosas

Para dar operatividad al SIGRIP, se sugiere documentar el siguiente flujo mínimo:

1. Detección: la primera línea identifica una operación que activa una o más señales de alerta y la reporta a la función de cumplimiento.
2. Análisis: la función de cumplimiento analiza la operación frente al comportamiento esperado del segmento y la información de la contraparte.
3. Decisión: si la operación se justifica, se documenta y archiva; si no, se califica como sospechosa.
4. Reporte: ante una operación sospechosa (incluida la intentada), se remite el ROS a la UIAF y, si hay lugar, se pone en conocimiento de la Fiscalía General de la Nación, con independencia de que se configure o no el delito.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

5. Conservación: se conservan los soportes por el término legal aplicable. El reporte no constituye prejuzgamiento ni denuncia.

Función de cumplimiento

La función de cumplimiento es el rol responsable de velar por el funcionamiento efectivo, eficiente y oportuno del SIGRIP en su conjunto y de cada uno de sus elementos. En la UPIT esta función es asumida por el Grupo Interno de Trabajo de Planeación —proceso Sistema Integrado de Gestión—, sin que ello implique la creación de un cargo independiente, y se formaliza mediante acto administrativo que precisa sus responsabilidades.

Para garantizar su adecuado ejercicio, la función de cumplimiento debe contar con independencia funcional, acceso a la información y un canal directo de reporte ante la Alta Dirección. Son responsabilidades de la función de cumplimiento, como mínimo:

- Velar por el funcionamiento del SIGRIP y de cada uno de sus componentes, y apoyar a los líderes de proceso y gestores de riesgo en su aplicación.
- Diseñar y mantener la metodología, las señales de alerta y los indicadores de riesgo para la integridad pública.
- Definir los criterios de debida diligencia en el conocimiento de las contrapartes y verificar su aplicación.
- Analizar las operaciones inusuales, calificar las sospechosas y remitir el respectivo Reporte de Operación Sospechosa (ROS) a la UIAF y, cuando haya lugar, a la Fiscalía General de la Nación.
- Promover la formación y la toma de conciencia sobre el SIGRIP y presentar a la Alta Dirección los resultados y las propuestas de mejora del Sistema.
- Conservar los documentos y registros de las contrapartes y sus operaciones por el término del artículo 12 de la Ley 2195 de 2022.

Canal de denuncias y protección al denunciante

La UPIT dispone de canales para recibir, evaluar, tramitar y cerrar denuncias o inquietudes asociadas a corrupción o a conductas contrarias a la integridad pública, articulados con el Programa de Transparencia y Ética Pública. Estos canales hacen parte de las herramientas de gestión del riesgo del SIGRIP y observan los siguientes lineamientos:

- Confidencialidad en el manejo de la identidad del denunciante y de la información reportada.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Protección al denunciante frente a represalias, conforme al marco legal aplicable.
- Posibilidad de presentar denuncias anónimas y registro trazable de su recepción, análisis y cierre.
- Remisión de los hallazgos a las autoridades o entes de control competentes (Fiscalía, Contraloría, Procuraduría o Control Interno Disciplinario) cuando corresponda.
- Uso de las denuncias como insumo de la base histórica de eventos y de la revisión de riesgos y controles.

15.Indicadores Clave de Riesgo

Los Indicadores Clave de Riesgo (*Key Risk Indicators* – KRI por sus siglas en inglés), surgen como una herramienta fundamental para la toma de decisiones informadas de cara a la mitigación de riesgos, por lo que a continuación se precisan sus bases conceptuales y orientaciones técnicas para su diseño que dependerá de las características y complejidad de la UPIT.

Tipologías de Indicadores para el seguimiento

Con el propósito de definir de forma adecuada los Indicadores Clave de Riesgo, es necesario enmarcarlos desde el despliegue de la plataforma estratégica de la entidad, la cual parte de la misión, visión y valores fundamentales, base para la formulación de los objetivos estratégicos, los cuales a su vez, no solamente orientan la planeación institucional, sino que también, permiten tener un despliegue hacia los objetivos de los procesos y se constituyen en la base para la identificación y formulación de Indicadores Clave de Desempeño *(Key Performance Indicators – KPI),* que hacen posible medir su cumplimiento.

En este sentido, de acuerdo con la estructura propuesta en la figura anterior se observa la forma como se vinculan los **Indicadores Clave de Riesgo** articulados con los **Indicadores Clave de Proceso.**

Por lo tanto, estos indicadores tienen una función principal que es monitorear los **riesgos clave que podrían afectar el cumplimiento de los objetivos y metas** establecidos durante las diversas etapas de la gestión institucional. Así mismo, son fundamentales para realizar ajustes en la operación cuando sea necesario, lo que permite asegurar que los riesgos sean gestionados de forma adecuada y las decisiones se tomen a tiempo para mitigar cualquier desviación o amenaza.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Alcance de los Indicadores Claves de Proceso y los Indicadores Clave de Riesgo

De acuerdo con la articulación explicada en el punto anterior, a continuación, se precisan los alcances en la aplicación de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI), ya que, si bien tienen diferencias, resultan complementarios en su análisis. A continuación, se presenta una tabla con las características de cada uno.

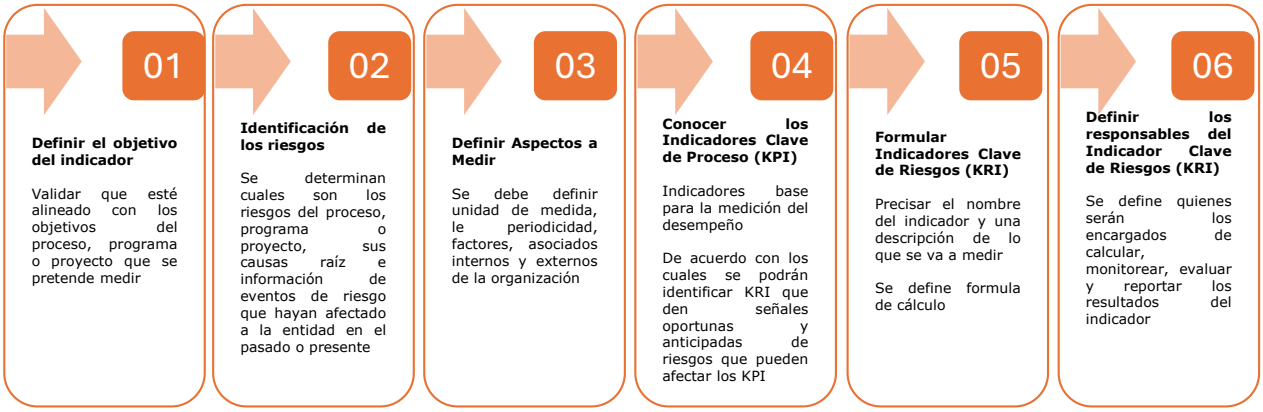
Indicadores Clave de Proceso (KPI)	Indicadores Clave de Riesgo (KRI)
Permiten medir periódicamente el desempeño general de la entidad y sus principales unidades operativas.	Complementan el seguimiento a los resultados de la entidad.
Se definen tomando como referencia las metas establecidas, por procesos, unidades u operaciones clave.	Proporcionan una señal temprana y oportuna de una exposición al riesgo en diversas áreas de la entidad.
Mide el rendimiento pasado, proporcionando información sobre qué tan bien se están logrando los objetivos estratégicos y operativos.	Proporcionan información útil sobre los riesgos emergentes y potenciales que pueden impactar en los objetivos estratégicos de la organización.
Ofrecen información sobre aquellos aspectos críticos de la operación que requieren mayores recursos y atención.	Ayudan a identificar y anticipar problemas que se pueden presentar interna o externamente, así como oportunidades futuras.
Permiten medir los resultados que se obtienen de la ejecución de los programas, planes y proyectos, en los diferentes momentos o etapas de su desarrollo.	Permiten realizar un monitoreo constante y mitigar los posibles eventos de riesgo que se presenten al aplicar medidas oportunas para disminuir su impacto.
Permiten mejorar la planificación, entender con mayor precisión las oportunidades de mejora de determinados procesos y analizar el desempeño de las acciones, logrando tomar decisiones con mayor certeza y confiabilidad.	Facilitan el proceso de generación de informes y el escalamiento de los riesgos.

Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

Para la definición y construcción de los Indicadores Clave de Riesgos (*KRI*), se proponen los siguientes pasos:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

Pasos para la construcción de Indicadores Clave de Riesgos (KRI)



Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

Para el desarrollo de los anteriores pasos se debe tener en cuenta:

Paso 1. **Definir el objetivo del indicador**, el cual debe estar alineado con los objetivos del proceso, plan, programa o proyecto que se pretende medir.

Paso 2. **Identificar los riesgos**, en este paso se determinan cuáles son los riesgos del proceso, plan, programa o proyecto, sus causas raíz e información de eventos de riesgo que hayan afectado a la entidad en el pasado o presente.

> Sobre la gestión de eventos, se trata de un riesgo materializado, donde se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente. Algunas fuentes para establecer una base histórica de eventos pueden ser: i) mesas de ayuda; ii) PQRD (peticiones, quejas, reclamos, denuncias); iii) Oficina jurídica; iv) Líneas internas y externas de denuncia.

Paso 3. **Definir los aspectos a medir**, para lo cual se deben establecer la unidad de medida, la periodicidad, los factores internos o externos de la entidad y especialmente, que se pretende medir.

Paso 4. **Conocer los Indicadores Clave de Proceso (*KPI*),** teniendo en cuenta que estos son la base de medición del desempeño del proceso, programa o proyecto.

Paso 5. **Formular el Indicador Clave de Riesgo (KRI)**, se debe precisar como mínimo lo siguiente:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- El nombre del indicador,
- una descripción de lo que se va a medir,
- la fórmula de cálculo,
- La fuente de información para el cálculo del indicador, por ejemplo: sistemas internos, reportes de auditoría, bases de datos internas y/o externas u otras fuentes,
- frecuencia de medición y seguimiento y;
- umbrales de alerta.

A continuación, se presentan algunos ejemplos de indicadores:

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

Fuente: Elaboración propia a partir de *Gestión Integral del Riesgo en Entidades Públicas Versión 7, DAFP, 2025*

Algunas recomendaciones a tener en cuenta para identificar y formular los Indicadores Clave de Riesgo (KRI) para una mayor efectividad se señalan a continuación:

✓ Relevancia: Deben estar alineados con los riesgos críticos para la entidad.
✓ Cuantificables: Es fundamental que los Indicadores Clave de Riesgo (KRI) puedan ser medidos de manera objetiva.
✓ Predictivos: Un buen Indicador Clave de Riesgo (KRI) debe ser capaz de predecir o bien detectar posibles problemas antes de que ocurran.
✓ Comparables: Los Indicadores Clave de Riesgo (KRI) deben permitir la comparación a lo largo del tiempo para identificar tendencias.

En cuanto a las limitaciones que pueden presentarse en el diseño de estos indicadores se tienen las siguientes:

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

✓ Un Indicador Clave de Riesgo (KRI) no sustituye la comprensión integral del contexto de la entidad, es decir, se requiere un conocimiento del entorno y las características de la entidad para diseñar y medir estos indicadores.

✓ Si la fuente de información (interna o externa) no es confiable porque esta desactualizada, es errada y/o no posee un histórico de datos podría ocasionar Indicadores Clave de Riesgo (KRI) ineficientes.

✓ Si presentan fallas en el establecimiento de los umbrales de los Indicadores Clave de Riesgo (KRI) puede generar que no se ajusten las estrategias de la entidad de manera proactiva y puede disminuir la probabilidad del cumplimiento de las metas y objetivos institucionales.

La aplicación de los Indicadores Clave de Riesgo para la UPIT se realizará una vez la entidad adelante el diagnóstico correspondiente, con el fin de identificar el estado actual de sus procesos, riesgos asociados y necesidades de seguimiento. A partir de dicho análisis, se definirán los indicadores pertinentes, su alcance, periodicidad y responsables, garantizando que su implementación responda a las condiciones reales de la entidad y contribuya al fortalecimiento de la gestión del riesgo institucional.

16. Conclusión

La administración del riesgo en la Unidad de Planeación de Infraestructura de Transporte — UPIT constituye un componente esencial para fortalecer la gestión institucional, la toma de decisiones, el cumplimiento de los objetivos estratégicos, la protección de los recursos públicos y la generación de confianza por parte de los grupos de valor y la ciudadanía. En este sentido, el presente Manual consolida los lineamientos estratégicos, metodológicos y operativos que orientan la identificación, análisis, valoración, tratamiento, monitoreo, revisión y mejora de los riesgos a los que se encuentra expuesta la Entidad, en concordancia con el Modelo Integrado de Planeación y Gestión — MIPG, el Modelo Estándar de Control Interno — MECI y la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, expedida por el Departamento Administrativo de la Función Pública — DAFP.

La actualización de este instrumento permite avanzar hacia una gestión del riesgo más integral, preventiva y articulada, en la cual los riesgos de gestión, fiscales, de seguridad de la información y aquellos asociados a la integridad pública son abordados de manera sistemática, bajo criterios comunes de análisis, control y seguimiento. Esta visión contribuye a que cada proceso de la Entidad reconozca sus puntos críticos, fortalezca sus controles, gestione oportunamente las causas que

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

pueden dar lugar a la materialización de riesgos y adopte acciones orientadas a preservar la legalidad, la eficiencia administrativa, la transparencia y el valor público.

De manera particular, la incorporación del Sistema de Gestión de Riesgos para la Integridad Pública — SIGRIP representa un avance significativo para la UPIT, en la medida en que amplía el enfoque tradicional de los riesgos de corrupción e integra amenazas como el soborno, el fraude, la inadecuada gestión de los conflictos de interés, el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva. Este enfoque permite fortalecer la cultura de integridad, promover comportamientos éticos, prevenir situaciones que puedan afectar la confianza institucional y consolidar mecanismos que faciliten la detección temprana, el reporte, el análisis y el tratamiento de posibles eventos contrarios a la función pública.

Así mismo, el Manual reafirma la importancia de la gobernanza del riesgo a través del esquema de líneas, en el cual la Alta Dirección, los líderes de proceso, los servidores públicos, contratistas, la segunda línea y la tercera cumplen roles diferenciados y complementarios. Esta articulación resulta fundamental para asegurar que la gestión del riesgo no sea entendida como una actividad aislada, sino como una responsabilidad compartida que debe estar integrada a la planeación institucional, a la operación cotidiana de los procesos, al seguimiento de los controles y a la mejora continua del Sistema Integrado de Gestión.

En este contexto, la UPIT continuará fortaleciendo los instrumentos de seguimiento en el marco del SIGRIP, mediante la mejora progresiva de sus mapas de riesgos, indicadores clave de riesgo — KRI, reportes de monitoreo, evidencias de ejecución de controles, análisis de eventos materializados, canales de comunicación, mecanismos de debida diligencia, gestión de conflictos de interés y herramientas de trazabilidad. Estos instrumentos permitirán contar con información más oportuna, confiable y útil para la toma de decisiones, así como identificar señales de alerta, tendencias, desviaciones y oportunidades de mejora frente a los riesgos que puedan afectar la integridad pública y el cumplimiento de los objetivos institucionales.

Finalmente, la implementación efectiva del presente Manual requiere el compromiso permanente de todos los niveles de la Entidad. Su apropiación por parte de los procesos, servidores públicos y contratistas permitirá consolidar una cultura basada en la prevención, el autocontrol, la transparencia, la responsabilidad, la integridad y la mejora continua. De esta manera, la UPIT fortalece su capacidad institucional para anticiparse a eventos adversos, responder oportunamente ante situaciones de

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

riesgo y garantizar una gestión pública orientada al cumplimiento de su misionalidad, la protección del interés general y el fortalecimiento de la confianza ciudadana.

17. Bibliografía

- Departamento Administrativo de la Función Pública — DAFP. (2025). *Guía para la Gestión Integral del Riesgo en Entidades Públicas. Versión 7*. Bogotá D.C., Colombia.
- Departamento Administrativo de la Función Pública — DAFP. (2024). *Manual Operativo del Modelo Integrado de Planeación y Gestión — MIPG. Versión 6*. Bogotá D.C., Colombia.
- Departamento Administrativo de la Función Pública — DAFP. (2025). *Anexo Glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas*. Bogotá D.C., Colombia.
- Departamento Administrativo de la Función Pública — DAFP. (2017). *Código de Integridad del Servicio Público Colombiano*. Bogotá D.C., Colombia.
- Departamento Administrativo de la Función Pública — DAFP. (s.f.). *Política de Integridad Pública en el marco del Modelo Integrado de Planeación y Gestión — MIPG*. Bogotá D.C., Colombia.
- Presidencia de la República de Colombia. (1991). *Constitución Política de Colombia*. Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (1993). *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*. Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (2011). *Ley 1474 de 2011, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública*. Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (2014). *Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional*. Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (2020). *Ley 2016 de 2020, por la cual se adopta el Código de Integridad del Servicio Público Colombiano y se dictan otras disposiciones*. Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (2022). *Ley 2195 de 2022, por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones*. Bogotá D.C., Colombia.

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

- Presidencia de la República de Colombia. (2015). *Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública*. Bogotá D.C., Colombia.
- Presidencia de la República de Colombia. (2017). *Decreto 1499 de 2017, por medio del cual se modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión y se actualiza el Modelo Integrado de Planeación y Gestión — MIPG*. Bogotá D.C., Colombia.
- Presidencia de la República de Colombia. (2017). *Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública*. Bogotá D.C., Colombia.
- Presidencia de la República de Colombia. (2022). *Decreto 338 de 2022, por el cual se establecen lineamientos generales para fortalecer la gobernanza de la seguridad digital*. Bogotá D.C., Colombia.
- Presidencia de la República de Colombia. (2024). *Decreto 1122 de 2024, por el cual se reglamentan los Programas de Transparencia y Ética Pública*. Bogotá D.C., Colombia.
- Ministerio de Tecnologías de la Información y las Comunicaciones — MinTIC. (2021). *Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información — MSPI*. Bogotá D.C., Colombia.
- Ministerio de Tecnologías de la Información y las Comunicaciones — MinTIC. (2025). *Resolución 02277 de 2025, por la cual se actualiza el Modelo de Seguridad y Privacidad de la Información — MSPI*. Bogotá D.C., Colombia.
- Ministerio de Tecnologías de la Información y las Comunicaciones — MinTIC. (2025). *Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional*. Bogotá D.C., Colombia.
- Consejo Nacional de Política Económica y Social — CONPES. (2020). *Documento CONPES 3995: Política Nacional de Confianza y Seguridad Digital*. Bogotá D.C., Colombia.

18. Anexos (Cuando aplique)

N-A

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA

19. Control de documentos

Versión Generada	Fecha	Descripción del Cambio o Modificación
01	02/08/2024	Versión Inicial del Documento
02	28/07/2026	Se mantiene estructura conceptual y metodológica general para la gestión del riesgo bajo un enfoque integral. Se define estructura general para la gestión integral del riesgo, con elementos comunes aplicables a todas las tipologías de riesgo. Se amplían términos y definiciones en concordancia con las actualizaciones en los capítulos, los cuales se desarrollan como anexo de la presente guía. Se incluyen contenidos del marco COSO-ERM (2017) que precisan y profundizan los conceptos de riesgo, gestión del riesgo y niveles de madurez del riesgo. En este marco general se profundiza el análisis sobre apetito del riesgo. Se incorpora un capítulo relacionado con la formulación de acciones de fortalecimiento y su seguimiento. Así mismo, de manera transversal se incluye a la herramienta para la implementación del sistema de gestión como instrumento de operación para la administración integral de los riesgos institucionales. Se modifica y actualiza el capítulo relacionado con riesgos asociados a posibles actos de corrupción, mediante la incorporación del Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP.

Elaboró	Revisó	Aprobó
Jorge Nicolás Olaya Mesa **Contratista Grupo Interno de Trabajo de Planeación.**	Johana Paola Lamilla Sánchez **Asesor Dirección General-Grupo Interno de Trabajo de Planeación**	Integrantes del Comité Institucional de Coordinación del Sistema de Control Interno **Sesión del 28 de julio de 2026**

La Unidad de Planeación de Infraestructura de Transporte declara como única documentación valida la ubicada en el Banco de Documentos, y entra en vigencia a partir de la publicación. Toda copia de este se declara COPIA NO CONTROLADA