PRESENTACION

La Superintendencia de Transporte, es la entidad encargada de supervisar la efectiva prestación del servicio público de transporte, su infraestructura y servicios conexos de forma incluyente, accesible y segura, propendiendo por el derecho fundamental a la vida y la protección a los usuarios, Tiene como visión para 2026 ser reconocida como una Entidad cercana e incluyente con sus grupos de valor e interés, a través, entre otros, del uso de tecnologías digitales, fomentando la legalidad, la construcción de la paz, la protección de los usuarios y la vida, en todo el territorio nacional.

En el marco del cumplimiento de su misión y visión ha definido tres objetivos estratégicos:

1. Implementar nuevas tecnologías con el fin de fortalecer los procesos de vigilancia, Inspección y Control – VIC como motor de cambio, para promover la confianza y el vínculo Estado-Ciudadanía.
2. Fortalecer la promoción y prevención para contribuir al fomento de la legalidad, la seguridad y la inclusión social, orientadas a la protección de los usuarios y la vida.
3. Mejorar la capacidad institucional aumentado la cobertura territorial para contribuir a la consolidación de la paz y la protección de los usuarios.

Para aportar al fortalecimiento institucional, la entidad tiene definida en su cadena de valor dieciséis (16) procesos, uno de ellos es el proceso de Direccionamiento Estratégico, cuyo objetivo es establecer lineamientos estratégicos y de operación en la Entidad, mediante procedimientos y metodologías de planeación y mejoramiento continuo, para el cumplimiento de los objetivos institucionales, sectoriales y metas del Plan Nacional de Desarrollo.

Por lo anterior, el proceso lidera la implementación metodológica de la Política para la Gestión Integral de Riesgos asumiendo que la gestión del riesgo es un factor determinante para que la Superintendencia pueda lograr sus objetivos mediante la identificación, análisis, evaluación y tratamiento del efecto de la incertidumbre.

El propósito del presente documento es el de actualizar el establecimiento del marco general de actuación de todos los actores de la entidad para la gestión integral de los riesgos, mediante la identificación de acciones de control, emisión de respuestas oportunas y formulación de estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro efectivo de objetivos institucionales, disminuyendo así las potenciales consecuencias negativas, y reduciendo las vulnerabilidades ante las amenazas internas y

externas; adicionalmente, permite mejorar las capacidades institucionales entorno a las respuestas a posibles eventos identificados o inesperados que afecten al equipo humano, la infraestructura tecnológica o servicios esenciales que a su vez generen impacto a los vigilados y la ciudadanía.

En este sentido, la Superintendencia de Transporte ha definido el marco de referencia que permite gestionar adecuadamente los eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos estratégicos y de los procesos, lo cual se representa en la presente Política para la Gestión Integral de Riesgos, siendo definida como la declaración de la dirección y las intenciones generales de la organización respecto a la gestión del riesgo[1], estableciendo lineamientos precisos acerca de la identificación, valoración, tratamiento, manejo y seguimiento a los riesgos.

La política que se desarrolla a continuación especifica los objetivos, alcance, definiciones, marco normativo, principios y responsabilidades teniendo en cuenta el Modelo Integrado de Planeación y Gestión - MIPG, que plantea el esquema de “Líneas de Defensa” para la gestión del riesgo, de este mismo modo, establece los niveles de aceptación del riesgo, define la forma en que se identifican, analizan y valoran los riesgos. Todo lo anterior, se enmarca en las directrices emitidas por el Departamento Administrativo de la Función Pública en la versión 7 en la “Guía para la Gestión Integral del Riesgo en Entidades Públicas”.

Se establecen los lineamientos para la administración de los riesgos de Gestión, Seguridad de la Información, Fiscales y Riesgos para la Integridad Pública. Con respecto a los Riesgos para la Integridad Pública se suministran las etapas de definición, valoración, monitoreo y seguimiento, de acuerdo con las directrices emitidas por la Secretaría de Transparencia de la Presidencia de la República, entidad que lidera la Política Pública de Transparencia, Integridad y Legalidad. Así como, la gestión de riesgos de seguridad de la información se basa en la Guía No. 7 de Gestión de riesgos del MINTIC.

Para la Superintendencia de Transporte la Política para la Gestión Integral de Riesgos representa la posición de la Alta Dirección frente al manejo de los Riesgos, en las que se fijan los lineamientos con relación a la Calificación de éstos, la forma de administrarlos y la protección de los recursos, estableciendo los parámetros para que todos los funcionarios y contratistas las apliquen al interior de los procesos. Esta política tiene un enfoque preventivo que permite la protección de los

[1] NTC ISO 31000:2011. Gestión del Riesgo. Principios y Directrices.

recursos públicos, el cumplimiento de los objetivos de la entidad y mejoramiento de la prestación de los servicios a la ciudadanía.

La actualización de la Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 que fue emitida durante el segundo semestre de la vigencia 2025, impulsa los siguientes aspectos:

I. Se mantiene la estructura conceptual y metodológica general para la gestión del riesgo bajo un enfoque integral, atendiendo las políticas de gestión y desempeño que se vinculan y su relación con otras políticas públicas y los sectores que las lideran.
II. Se define una estructura de administración general para la gestión integral del riesgo, con elementos comunes aplicables a todas las tipologías de riesgo.
III. Se amplían los términos y definiciones en concordancia con la aplicación de los nuevos elementos.
IV. Se profundiza el análisis sobre apetito del riesgo en el marco COSO-ERM (2017) que precisa y profundiza los conceptos de riesgo, gestión del riesgo y niveles de madurez del riesgo.
V. Se precisan contenidos conceptuales y ejemplos relacionados con la gestión preventiva de riesgos fiscales.
VI. Se modifica y actualiza el capítulo de riesgos asociados a posibles actos de corrupción, incorporando el Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, de acuerdo con el componente programático de la Estrategia Institucional para la Lucha Contra la Corrupción, temática 1 Administración del Riesgo indicado en el Anexo Técnico de los Programas de Transparencia y Ética Pública.
VII. Se actualizan contenidos relacionados con los riesgos de seguridad de la información, desplegando la totalidad de los pasos metodológicos.

TABLA DE CONTENIDO

PRESENTACION ..... **¡Error! Marcador no definido.**
1. OBJETIVO GENERAL 7
2. OBJETIVOS ESPECÍFICOS 7
3. ALCANCE 8
4. DEFINICIONES 8
5. MARCO NORMATIVO 9
6. RESPONSABILIDADES 9
6.1 Línea Estratégica 9
6.1.1 Comité Institucional De Gestión y Desempeño. 10
6.1.2 Comité Institucional De Coordinación De Control Interno 10
6.2 Líneas De Defensa 10
7. DECLARACIÓN DE LA POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS 13
8. LINEAMIENTOS DE POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS 14
8.1 Determinación del Nivel de madurez 15
8.2 Metodología para la Gestión Integral del Riesgo 16
8.3 Apetito, Tolerancia y Capacidad del Riesgo. 17
8.4 Identificación de riesgos. 19
8.4.1 Clasificación del Riesgo por Factor 23
8.5 Identificación de áreas de impacto 25
8.6 Identificación de áreas de factores de riesgo 25
8.7 Estructura de la descripción del Riesgo 27
8.7.1 Análisis De Riesgo Inherente 28
8.7.2 Zonas de severidad 30
8.8 Diseño, Análisis y Valoración de Controles 31

8.8.1 Diseño de controles 33
8.8.2 Aplicación de controles y riesgo residual 37
8.9 Tratamiento del Riesgo 38
8.10 Consolidación en el mapa de riesgos. 39
8.10.1 Inactivación de un riesgo. 40
9. TIPOLOGÍAS DE RIESGO 40
9.1 Riesgos de Gestión. 40
9.1.1 Monitoreo y seguimiento. 42
9.1.2 Materialización de riesgos. 43
9.1.3 Materialización de riesgos no identificados. 44
9.2 Riesgos de Seguridad de la Información. 44
9.2.1 Identificación de los activos de seguridad de la información. 45
9.2.2 Identificación de Riesgos de Seguridad de la información. 46
9.2.3 Consolidación en el Mapa de Riesgos 50
9.2.4 Monitoreo y seguimiento. 50
9.2.5 Materialización de riesgos. 52
9.3 Riesgos Fiscales 53
9.3.1 Identificación de áreas de factores de riesgo 53
9.3.2 Identificación del Riesgo 54
9.3.3 Identificación de Puntos de Riesgo Fiscales y Causa Inmediata 54
9.3.4 Identificación de áreas de impacto 55
9.3.5 Identificar el efecto económico 56
9.3.6 Identificación de la causa raíz o potencial hecho generador 57
9.3.7 Descripción del Riesgo Fiscal 57
9.3.8 Monitoreo y seguimiento. 60
9.3.9 Materialización de riesgos. 62
9.3.10 Materialización de riesgos no identificados. 63

9.4 Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP 63
9.4.1 Integridad pública 64
9.4.2 Amenazas para la integridad pública. 65
Soborno 65
Fraude 65
Conflicto de intereses 65
Corrupción 66
Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) - LA/FT/FP 66
9.4.3 Operación del SIGRIP 66
9.4.4 Identificación de riesgos. 68
9.4.5 Identificación de áreas de impacto 68
9.4.6 Identificación de áreas de factores de riesgo. 69
9.4.7 Estructura de la Descripción del riesgo. 70
9.4.8 Monitoreo y seguimiento. 71
9.4.9 Materialización de riesgos. 73
9.4.10 Materialización de riesgos no identificados. 74
10. INDICADORES (KRI) 74
11. CONTROL Y SEGUIMIENTO 75
12. CONTROL DE CAMBIOS DEL DOCUMENTO 75
ANEXO 1 76

1. OBJETIVO GENERAL

Establecer los lineamientos estratégicos, el marco general y operativo que orienten la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos en la Superintendencia de Transporte que puedan afectar el logro de los objetivos institucionales, en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG) y las mejores prácticas internacionales de gestión de riesgos basadas en el marco COSO ERM.
Es propósito de esta política es de fortalecer la gobernanza, la toma de decisiones informadas y la generación de valor público, preservando la integridad, transparencia y eficiencia en la administración de recursos. Igualmente, busca promover una cultura organizacional orientada a la anticipación y gestión proactiva de riesgos, contribuyendo al cumplimiento de la misión institucional, la mejora continua, la confianza ciudadana y la protección de la integridad pública.

Lo anterior contemplando la relación con los diferentes grupos de valor con los que la entidad se relaciona, especialmente las contrapartes; las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización; los procesos, servicios, trámites u otras operaciones administrativas de la organización, especialmente aquellas que implican alguna interacción y las jurisdicciones o territorios donde se opera.

2. OBJETIVOS ESPECÍFICOS

- Establecer los lineamientos para la gestión integral de los riesgos en los procesos de la entidad, así como los niveles de aceptación del riesgo, con el fin de mitigar los efectos ante la posibilidad de su materialización.
- Establecer las directrices para la identificación, valoración, monitoreo y seguimiento de los riesgos de Gestión, Seguridad de la Información, Fiscales y Riesgos para la Integridad Pública.
- Brindar criterios para la estructuración de controles que reduzcan o mitiguen los riesgos identificados evitando su materialización.
- Definir criterios para actuar de manera oportuna ante la materialización de los riesgos identificados.
- Impulsar el reporte y análisis oportuno de los riesgos, así como la implementación de controles y acciones preventivas que permitan anticipar situaciones potenciales y responder con agilidad.
- Mejorar el direccionamiento estratégico de la entidad.

- Apoyar la toma de decisiones y la planificación en función de la gestión basada en riesgos.
- Fomentar una cultura de integridad que guíe el actuar diario de todos nuestros colaboradores hacia la transparencia, la responsabilidad y el servicio a la ciudadanía
- Gestionar los riesgos de seguridad de la información, con el fin que se prevengan o reduzcan efectos indeseados en los activos de información y se consideren oportunidades que permitan el mejoramiento continuo.
- Brindar criterios para la estructuración de riesgos y controles de eventos considerados como materializados no identificados que afecten el cumplimiento de los objetivos de los procesos.

3. ALCANCE

La Política de Gestión Integral del Riesgo de la Superintendencia de Transporte aplica a todas las dependencias, procesos, servidoras, servidores de la entidad en todos los niveles jerárquicos y áreas misionales, estratégicas y de apoyo, así como a los contratistas y terceros que ejecuten actividades en su nombre. Comprende la gestión de riesgos en el direccionamiento estratégico, la planeación, ejecución presupuestal, prestación de servicios, trámites administrativos, adopción de tecnologías, fortalecimiento organizacional, y la implementación de proyectos, programas y sistemas de gestión institucionales.

En cuanto al contexto organizacional, la política considera las relaciones con los diferentes grupos de valor con los que la Superintendencia interactúa, incluyendo empresas vigiladas del sector transporte terrestre, aéreo, férreo, marítimo y fluvial; usuarios del servicio de transporte; entidades del Estado y organismos de control; autoridades territoriales; gremios y asociaciones del sector; proveedores y contratistas. Reconoce la relación de adscripción al Ministerio de Transporte y el control que ejerce sobre las entidades del sector bajo su competencia. La política opera donde la entidad ejerce sus funciones de inspección, vigilancia y control, articulándose con el Sistema de Control Interno bajo el enfoque de las tres líneas de defensa.

4. DEFINICIONES

DE-GL-001

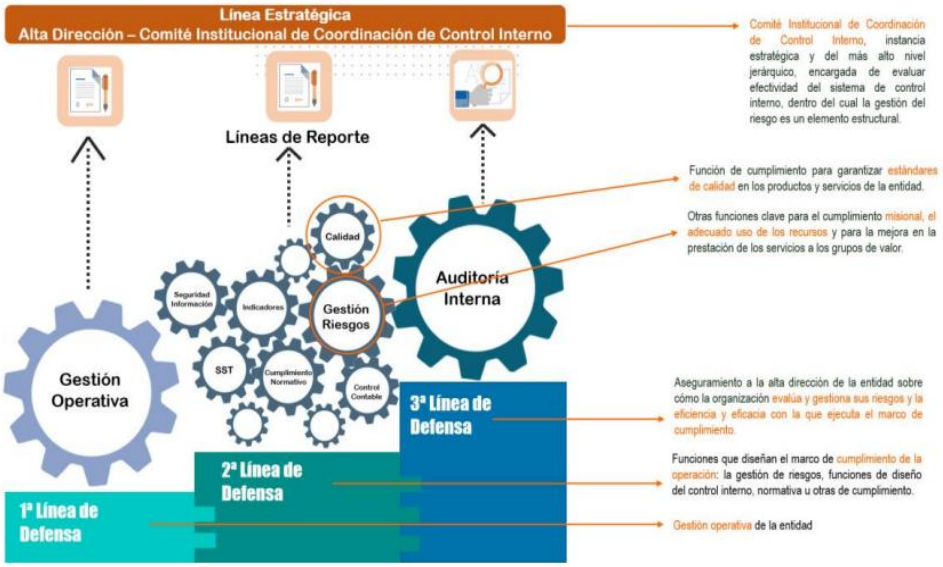
Glosario Direccionamiento Estratégico [Ver. 001 // Rev. 01 // FV. 2025-10-24]

5. MARCO NORMATIVO

Normograma_Direccionamiento_Estrategico.xlsx

6. RESPONSABILIDADES

Ilustración 1. Roles y responsabilidades de las líneas de defensa.



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Versión 6. 2022.

Las actividades que deben ser realizadas por las líneas de defensa para la adecuada gestión de riesgos en la Superintendencia de Transporte son:

6.1 Línea Estratégica

Se compromete con definir, aprobar, evaluar y dar línea a la Política para la Gestión Integral de Riesgos, en el marco del Comité Institucional de Gestión y Desempeño - CIGD. Debe aplicar el monitoreo a la Gestión del Riesgo como mínimo dos veces al año, haciendo uso de la información suministrada periódicamente por la 2a y 3ª línea de defensa, con lo cual toma decisiones y acciones necesarias para intervenir en los distintos eventos o escenarios que se puedan presentar, evitando que se generen incumplimientos, retrasos e incluso posibles actuaciones irregulares propendiendo el cumplimiento de los objetivos de los procesos y de la entidad. En

especial, si se han presentado materializaciones de riesgo debe efectuar seguimiento a las acciones planteadas en la presente política.

6.1.1 Comité Institucional De Gestión y Desempeño.

El Comité se encarga de orientar la implementación y funcionamiento del MIPG. Para ello, desarrolla funciones clave que influyen directamente en la gestión de riesgos, como:

- Aprobar y hacer seguimiento a las estrategias del MIPG, incluida la política de gestión de riesgos, y promover su actualización periódica.
- Coordinar esfuerzos institucionales y alinear recursos y metodologías para fortalecer el MIPG, integrando el análisis de riesgos en la planeación estratégica y en la definición de objetivos, metas y niveles de riesgo aceptables.
- Realizar y fomentar autodiagnósticos permanentes, definiendo mecanismos y responsables para monitorear los resultados de la gestión de riesgos y usar esta información para orientar decisiones estratégicas y acciones de mejora

6.1.2 Comité Institucional De Coordinación De Control Interno

Este comité contribuye a la gestión de riesgos mediante funciones como:

- Evaluar y fortalecer el Sistema de Control Interno, aprobando sus ajustes y mejoras.
- Aprobar y hacer seguimiento al Plan Anual de Auditoría, garantizando que cubra los proyectos estratégicos y las áreas críticas según el análisis de riesgos realizado por Control Interno.
- Resolver diferencias y conflictos de interés que puedan afectar la independencia o el desarrollo de la auditoría interna.
- Presentar para aprobación la política de administración del riesgo del representante legal y supervisar su aplicación, especialmente en lo relacionado con la prevención y detección del fraude y la mala conducta.
- Verificar que las líneas de defensa funcionen adecuadamente, asegurando una gestión del riesgo integral y articulada en todos los niveles de la entidad.

6.2 Líneas De Defensa

El siguiente es el complemento de la actuación de las líneas de defensa restantes:

Tabla 1. Actividades de las líneas de defensa.

Desde la 1ª línea de defensa todos los servidores públicos tienen la responsabilidad frente a la identificación y valoración de riesgos, así como la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores públicos con personal a cargo, por lo cual corresponde a los Líderes de Proceso y enlace MIPG asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades. Así como: - Debe garantizar la ejecución de los controles contando con evidencia objetiva, permitiendo el monitoreo y revisión periódica; en caso de ser necesario algún ajuste debe coordinar dicha gestión con la Segunda Línea Defensa del proceso. - Será su responsabilidad dar reporte de la materialización de los riesgos a la Segunda y Tercera línea de Defensa, así como, el cumplimiento del reporte y cargue de evidencias en los repositorios de información destinados para ello en los tiempos estipulados por la Oficina Asesora de Planeación. - El Rol de Gestor de Riesgos será desempeñado por el enlace MIPG de cada proceso. - Le corresponde la ejecución y el monitoreo de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.
Desde la 2ª línea de defensa, a cargo de la Oficina Asesora de Planeación, encargada de ejecutar la consolidación de la gestión del riesgo, así como la difusión y asesoría de la presente metodología, junto al tratamiento de los riesgos identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación. A su vez debe: - Capacita, acompaña, asesora y recomienda con base a los lineamientos definidos en el presente documento, la metodología suministrada por el Departamento Administrativo de la Función Pública y la norma técnica NTC-ISO 31000. - El Jefe de la Oficina Asesora de Planeación y su Equipo o quien esté encargado debe periódicamente hacer un seguimiento a todas las tipologías de riesgos (Gestión, Seguridad de la Información, Fiscales y Riesgos para la Integridad Pública), permitiendo evidenciar los cambios, avances e incumplimientos que se generen, así como la coordinación de los posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea de defensa pueden reflejar las mejoras a los riesgos y controles.

- Para el caso de los riesgos de seguridad de la información la Oficina de Tecnologías de la Información y Comunicaciones realizará la asesoría correspondiente en la identificación y análisis, así como del seguimiento de los planes sobre la implementación de controles definidos en cada uno de los riesgos identificados.
La 3ª línea de defensa que corresponde a la Oficina de Control Interno - OCI, a través de sus informes de auditorías, evaluaciones o seguimientos aprobado en el Plan Anual de Auditorías – PAA de la vigencia actual por el Comité Institucional de Coordinación de Control Interno – CICCI, deben realizar el seguimiento de los controles de los riesgos definidos en el Mapa de Riesgos del correspondiente proceso. A su vez debe: - Dar a conocer a la entidad los resultados del informe de auditoría, evaluación o seguimiento de la gestión del riesgo. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina Asesora de Planeación - OAP. - Debe asesorar cuando sea requerida en compañía de la Oficina Asesora de Planeación y la Oficina de Tecnología de la Información y las Comunicaciones - OTIC, a la primera línea de defensa en el análisis valoración del riesgo, y en el diseño de los controles. - Verificar la publicación del mapa de riesgos en el portal web institucional. - Realizar seguimiento a la gestión de riesgos (analizar causas, riesgos, eficacia y efectividad de los controles). - Recomienda mejoras a la Política para la Gestión Integral de Riesgos. - Auditar el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP y el cumplimiento de la presente política, así como sus complementos, con el propósito de asesorar y recomendar mejoras con un enfoque basado en riesgos.

Fuente: Elaboración propia.

OFICINA ASESORA DE PLANEACIÓN.

- Proponer en el Comité Institucional de Coordinación de Control Interno - CICCI la Política para la Gestión Integral de Riesgos, las modificaciones o actualizaciones del lineamiento.
- Coordinar la implementación de la Política para la Gestión Integral de Riesgos.
- Efectuar monitoreo al cumplimiento de los lineamientos definidos en la Política para la Gestión Integral de Riesgos.

- Presentar al Comité Institucional de Coordinación de Control Interno - CICCI el resultado obtenido en los seguimientos y monitoreos periódicos.

7. DECLARACIÓN DE LA POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

La Superintendencia de Transporte asume el compromiso de administrar los Riesgos de Gestión, Seguridad de la Información, Fiscales y Riesgos para la Integridad Pública; que puedan afectar de manera negativa el alcance de su misión, objetivos estratégicos y los objetivos de los procesos de la entidad, suministrando los recursos que sean necesarios para su operación; además de forjar una entidad preventiva, proactiva y detectiva en lugar de reactiva y correctiva, que trabaje en la reducción de los efectos no deseados y promoviendo la mejora continua, proyectando así, una organización basada en la acción preventiva automática, que controla todos los procesos de la entidad, brindando seguridad razonable, destinando los esfuerzos y recursos necesarios para administrar los riesgos y la definición de la ruta estratégica y operativa con el propósito de satisfacer las necesidades de los grupos de valor.

La Superintendencia de Transporte como entidad encargada de supervisar la efectiva prestación del servicio público de transporte, su infraestructura y servicios conexos de forma incluyente, accesible y segura, propendiendo por el derecho fundamental a la vida y la protección a los usuarios, mediante la Política para la Gestión Integral de Riesgos se compromete a:

- Establecer y apropiar la responsabilidad al interior de la Superintendencia de Transporte en todos los niveles de la organización con el propósito de identificar, valorar, controlar, prevenir y monitorear los riesgos de manera oportuna y efectiva.
- Identificar y tratar los riesgos de seguridad de la información tomando como insumo los activos de información de cada proceso y su clasificación según su nivel de a nivel de criticidad.
- Diseñar y ejecutar controles eficaces y alineados con las mejores prácticas para evitar la materialización de riesgos y si esto ocurre, asegurar la actuación correctiva y oportuna para mitigar las posibles consecuencias a fin de mantener niveles de riesgo aceptables.
- Asignar, establecer y disponer los recursos técnicos, tecnológicos, financieros y el talento humano necesarias, con la participación de los servidores públicos y contratistas, para gestionar, controlar y responder a los acontecimientos potenciales o aquellos que puedan desencadenar la materialización de los riesgos.
- Realizar monitoreo de los riesgos, así como efectuar seguimiento y evaluación sistemática para asegurar que la gestión del riesgo sea efectiva y permita la toma de decisiones informadas y la mejora continua.

A través de esta política la Superintendencia de Transporte busca promover una cultura de integridad que oriente la actuación de todos los colaboradores hacia la transparencia, la responsabilidad y el servicio al interés general, para alcanzar los objetivos estratégicos y de los procesos, proteger los recursos públicos y generar valor público en la prestación de los servicios a la ciudadanía a través de la mejora continua.

8. LINEAMIENTOS DE POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

Para el desarrollo de una óptima gestión del riesgo la entidad adopta la estructura sugerida por COSO-ERM-2017 (*Committee of sponsoring organizations of the treadway Commission – Enterprise Risk Management* por sus siglas en inglés), descrita en la "*Guía para la Gestión Integral del Riesgo en Entidades Públicas"* versión 7 del Departamento Administrativo de la Función Pública, que manifiesta 5 componentes que integran la óptima gestión del riesgo y son desarrollados de la siguiente a continuación:

a. Gobierno y Cultura:

Son la base de los demás componentes, mediante el gobierno se indican los lineamientos, manifestando la importancia y suministrado los roles y responsabilidades frente a la gestión integral del riesgo. La cultura es reflejada en la toma de decisiones al interior de la entidad dados los monitoreos y seguimientos.
Para lo anterior desde el Comité Institucional de Coordinación de Control Interno – CICCI se ejercerá la supervisión de la gestión integral del riesgo, se debe cumplir con la estructura operativa descrita en el capítulo 6 "Responsabilidades", la cultura deseada se obtiene dada la aplicación de la presente Política frente a la gestión del riesgo, se desarrollan el compromiso con los valores clave descritos en el numeral 7. "Principios de la Política", y propende la atracción, desarrollo y retención de profesionales capacitados.

b. Estrategia y establecimiento de Objetivos:

La gestión integral del riesgo confluye con el plan estratégico de la entidad a través del establecimiento de la estrategia y de los objetivos de la entidad. Con un conocimiento profundo del contexto y de los procesos, se comprenden los factores internos y externos y sus efectos en el riesgo. En su desarrollo se analiza el contexto, se logra la definición del apetito del riesgo, se evalúan las estratégicas de gestión y se formulan los objetivos del negocio.

c. Desempeño

La entidad identifica y evalúa los riesgos que pueden afectar su capacidad para alcanzar los objetivos estratégicos y de proceso. Motivo por el que se establecen las respuestas a los eventos de riesgo y efectúa monitoreo y seguimiento al desempeño considerando posibles cambios mediante la toma de decisiones. En su desarrollo se efectúa la identificación de los riesgos, se evalúa su gravedad estableciendo prioridades, así como implementando respuesta ante los eventos fortaleciendo la visión de la gestión.

d. Revisión y monitorización

La entidad examina sus capacidades y lineamientos respecto a la gestión integral del riesgo, así como su desempeño en relación con sus objetivos permitiéndose evaluar los cambios significativos, revisando los eventos y los resultados de sus seguimientos, promoviendo la mejora.

e. Información, comunicación y reporte

Corresponde al proceso continuo e iterativo de obtener y compartir información en toda la entidad. La Alta Dirección utiliza información obtenida por los informes de monitoreo y seguimiento (fuentes internas) y los suministrados por auditorías externas para facilitar la gestión integral del riesgo. La entidad aprovecha los sistemas de información para capturar, procesar y gestionar datos e información. Al utilizar información que se aplica a todos los componentes, la organización informa sobre el riesgo, la cultura y el desempeño.

8.1 Determinación del Nivel de madurez

Para determinar el nivel de madurez se deben evaluar los componentes y los principios descritos previamente y reflejados en la tabla 2, ejercicio que obtiene asignando una calificación de 1 a 5 para cada uno de los principios, permitiendo obtener el grado de madurez para la gestión integral del riesgo en la entidad. Para el desarrollo del ejercicio se cuenta con el “Autodiagnóstico madurez Gestión Integral del Riesgo”, herramienta suministrada por el Departamento Administrativo de la Función Pública y que es apropiado por la entidad que consolida los resultados por componente y genera un mapa de calor, donde se resaltan los temas a intervenir en una escala de severidad o prioridad para atención, de tal manera que la Oficina Asesora de Planeación informa a la Alta Dirección en el CICCI las orientaciones o acciones que desde allí deben surgir para garantizar la gestión integral del riesgo en la entidad.

Tabla 2. Componentes y principios evaluables modelo de madurez

Componente	Principios
Gobierno y Cultura	Supervisión de riesgos a través del consejo de administración
	Establece estructuras operativas
	Define la cultura deseada
	Demuestra compromiso con valores clave
	Atrae, desarrolla y retiene a profesionales capacitados
Establecimiento de la estrategia y objetivos	Analiza el contexto (externo e interno)
	Define el apetito del riesgo
	Evalúa estrategias alternativas
	Formula objetivos estratégicos y operacionales
Desempeño	Identifica y describe el riesgo
	Evalúa el riesgo inherente
	Diseña controles efectivos
	Prioriza riesgos
	Desarrolla visión integral
Análisis y monitorización	Evalúa los cambios significativos
	Revisa el riesgo y el desempeño
	Persigue la mejora de la gestión del riesgo
Información, Comunicación y Reporte	Aprovecha la información y la tecnología
	Comunica información sobre riesgos
	Informa sobre el riesgo, la cultura y el desempeño

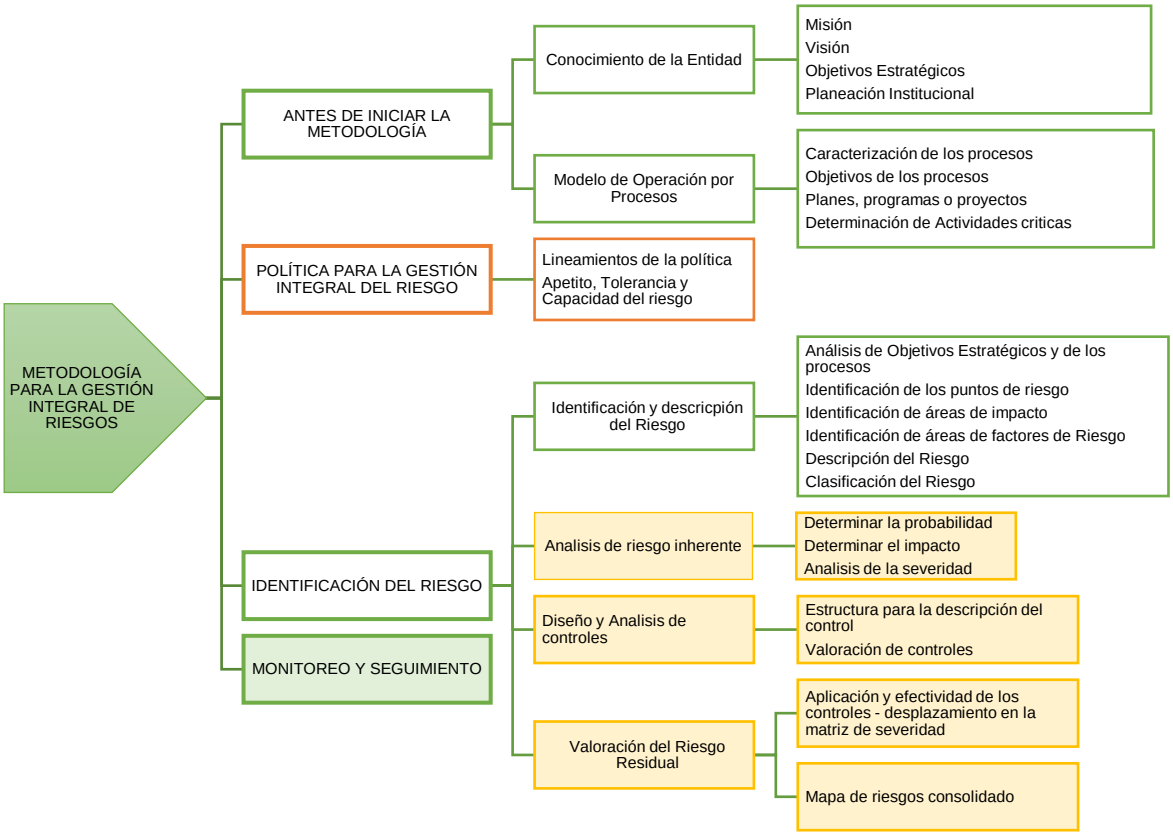
Fuente: Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025.

El análisis sobre niveles de madurez debe desarrollarse una vez al año.

8.2 Metodología para la Gestión Integral del Riesgo

Para la adecuada gestión integral del Riesgo la Superintendencia de Transporte establece el desarrollo de las siguientes etapas que son desarrolladas en la presente política:

Ilustración 2. Metodología para la Administración de Riesgos

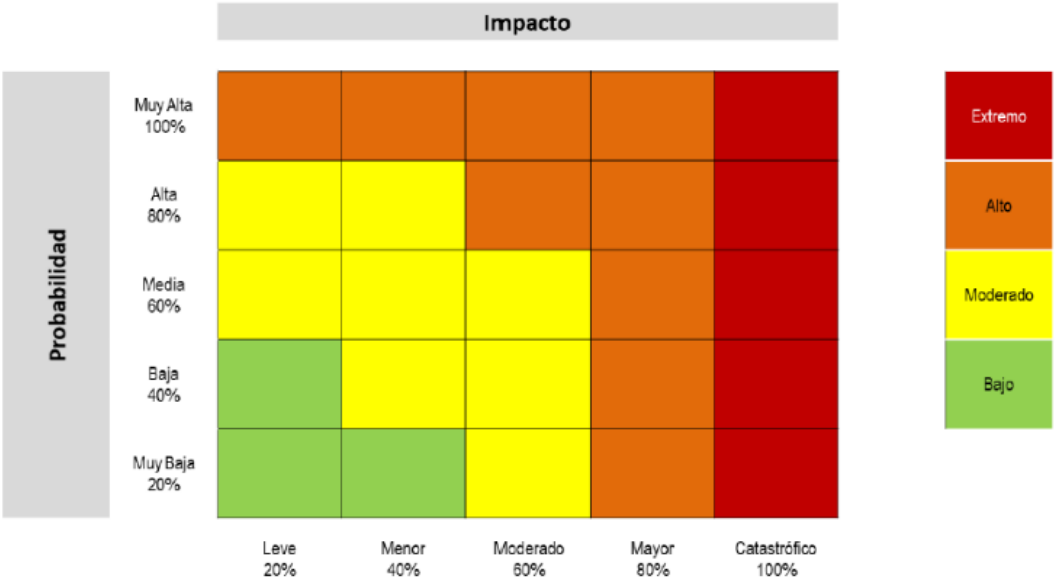


Fuente: Elaboración propia OAP.

8.3 Apetito, Tolerancia y Capacidad del Riesgo.

Para ilustrar el Apetito del Riesgo, Tolerancia del Riesgo y Capacidad del Riesgo determinado por la entidad es necesario revisar gráficamente el Nivel del Riesgo en el mapa de calor, lo cual se detalla a continuación:

Ilustración 3. Mapa de Calor de Riesgos.



Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025.

Para ello, es necesario aclarar que la entidad hace uso del mapa de calor sugerido por Función Pública, en este el Nivel del Riesgo 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. Dado lo anterior, se establece lo siguiente:

Apetito del Riesgo: Nivel de Riesgo **Bajo**.
Tolerancia del Riesgo: Desde nivel de Riesgo **Moderado** hasta Nivel de Riesgo **Alto**.
Capacidad de Riesgo: Nivel de Riesgo **Extremo**.

La Alta Dirección considera que el nivel de riesgo extremo es el valor máximo que, podrá ser resistido por la entidad, manteniendo la capacidad de cumplir con sus objetivos trazados. En caso de evidenciar eventos de riesgo que sobrepasen el nivel de riesgo extremo requerirán su replanteamiento incluyendo la posibilidad de definir nuevos valores de probabilidad e impacto.

Nota: En todo caso para los riesgos identificados e incluidos en las matrices de Riesgos se deben formular acciones de tratamiento.

8.4 Identificación de riesgos.

Son varios los insumos para efectuar la identificación de riesgos, dentro de los elementos que se deben tener en cuenta se encuentran los siguientes: el contexto estratégico en el que opera la entidad y los procesos contemplando los factores internos y externos, la caracterización de cada proceso y el desarrollo de sus actividades críticas contemplando su objetivo y alcance, el inventario de activos de información para la identificación de riesgos de seguridad de la información, la revisión del historial de hallazgos de incidencia fiscal y la identificación de puntos de riesgo fiscal para la gestión de riesgos fiscales, y finalmente el análisis de los objetivos estratégicos de la entidad y del proceso.

Se debe aplicar el uso de al menos uno de ellos, sin embargo, para poder establecer una adecuada identificación del Riesgo dichos elementos deben combinarse.

A) Análisis de Factores de Riesgo

En esta etapa se deben tener en cuenta:

- **Contexto externo:** Se examinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:
    - Políticos.
    - Económicos y financieros.
    - Sociales y culturales.
    - Tecnológicos.
    - Ambientales.
    - Fiscal.
    - Legales y reglamentarios.
    - Grupos de interés externos y partes interesadas.
    - Clientes, proveedores de servicio y empresas.
    - Cantidad de ciudadanos afectados por la falta del servicio.
    - Suplantación de identidad.
    - Asaltos/Vandalismo/Ataque terrorista/Orden Público a las instalaciones de la entidad.
    - Resultados de las evaluaciones llevadas a cabo por los organismos de control.

- **Contexto interno:** Se analizan cuáles son los rasgos distintivos que dictan la manera en la cual opera internamente y busca alcanzar sus objetivos institucionales:
    - Sector.
    - Misión.
    - Visión.
    - Valores.
    - Estructura organizacional.
    - Funciones y responsabilidades.
    - Políticas, procesos y procedimientos. Objetivos y estrategias implementadas.
    - Sistema de gestión.
    - Recursos y conocimientos con que se cuenta (económicos, social, ambiental, físico, financiero, jurídico, Humano, procesos, sistemas, infraestructura física y tecnológica, información, Seguridad Digital).
    - Relaciones con las partes involucradas y grupos de valor.
    - Cultura organizacional.
    - Infraestructura.
    - Tramites u otros procedimientos administrativos - OPA´S (Corrupción).
    - Resultados de las evaluaciones llevadas a cabo por la OCI.

- **Contexto del Proceso:** Se revisan cuáles son las características o aspectos esenciales del proceso, si está directamente relacionado con un objetivo estratégico de la entidad, cuál es su alcance, cuáles son las entradas y las salidas derivadas de las actividades que se realizan en su interior:

    - Objetivo del proceso.
    - Alcance del proceso.
    - Caracterización del proceso.
    - Interrelación con otros procesos.
    - Procedimientos asociados.
    - Responsables del proceso.
    - Cantidad de ciudadanos afectados por el proceso.
    - Procesos de gestión de riesgos actualmente implementados.
    - Actividades criticas

- **SIGRIP:** En cumplimiento a la implementación se deben realizar los siguientes análisis:

    - La planta y estructura de la entidad, así como la delegación de autoridad o poder decisorio discrecional. *

- Los grupos de valor o partes interesadas, incluidos los clientes internos y externos, permitiendo la identificación de contrapartes, es decir, partes con las que se tienen interacciones, entendidas estas como cualquier tipo de vinculación que involucre la prestación o entrega de un producto, o el intercambio de recursos.
- Identificar los lugares en qué opera la entidad.
- La naturaleza, escala y complejidad de los procesos, servicios, trámites u otras operaciones administrativas de la organización, así como las interacciones, es decir, las operaciones con contrapartes que involucran la prestación o entrega de un producto, o el intercambio de recursos.
- Segmentar la información general de los contratos y principales proveedores de la entidad. Agrupar los contratos y proveedores según sus características: naturaleza jurídica, modalidad de selección más recurrente, valores mínimos, máximos y media de contratación, relación de cumplimiento o incumplimientos, tipos de supervisión, entre otras.
- Identificar las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización. *
- La naturaleza y alcance de las interacciones con entidades de otras Ramas del Poder Público, órganos de control o independientes. Así como de las interacciones con particulares que no derivan en un vínculo formal, pero que son recurrentes (actividades de cabildeo). *
- Las obligaciones generales de la entidad, con independencia de la fuente: legal, reglamentaria, contractual, extracontractual u obligaciones profesionales. Agrupando entre aquellas que son deberes (obligatorio cumplimiento), expectativas (cumplimiento facultativo) y compromisos (cumplimiento asumido). *

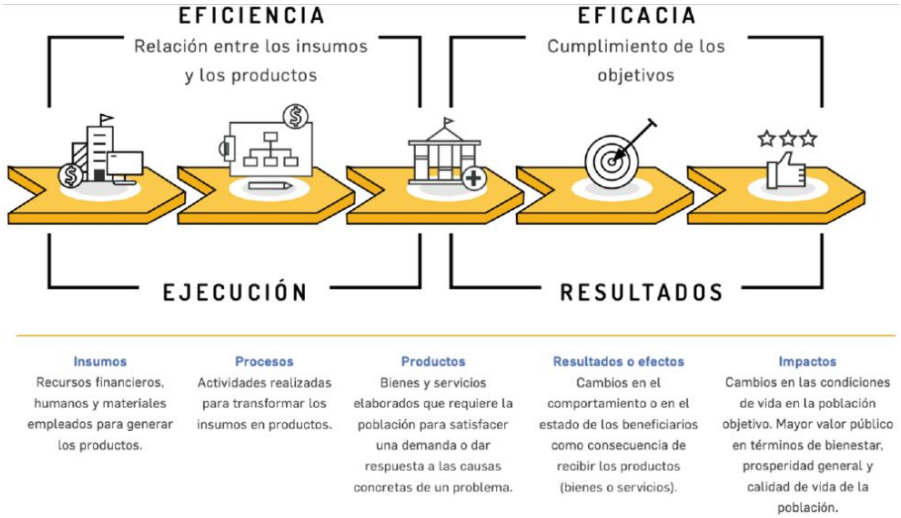
* Desarrollado en el marco de la temática de Redes y Articulación del Programa de Transparencia y Ética Pública.

Hace parte integral de la política el análisis de contexto interno y externo realizado en la vigencia

B) Identificación y análisis de las actividades críticas del proceso

Dado que los objetivos estratégicos y de proceso se alcanzan por medio de la ejecución de actividades, en esta etapa se busca identificar las situaciones cruciales para la consecución de los objetivos validando la integridad de la caracterización del proceso y los procedimientos que lo componen, lo anterior es lo que se denomina Puntos de Riesgo dentro de la cadena de valor.

Ilustración 4. Cadena de valor.



Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025.

De este modo, para establecer los puntos de riesgo clave en los procesos, es necesario considerar los atributos asignados a los productos, servicios o resultados de cada proceso y que podrían verse afectados dentro del ciclo del proceso que se esté analizando, así como el efecto de estos posibles eventos en el resultado de otros procesos, dentro de la cadena de valor.

C) Análisis de los Objetivos Estratégicos y de los Procesos

En una correcta construcción de objetivos por procesos se debe tener en cuenta la correlación que debe existir entre los objetivos estratégicos de la entidad y éstos, teniendo en cuenta el cumplimiento y cualquier situación que pueda representar su éxito o fracaso, a su vez, los objetivos estratégicos deben estar alineados con la misión y visión de la entidad. Lo anterior, permite una apropiada gestión de planeación en la identificación del riesgo en función de la afectación al logro y su posible fracaso impactando los propósitos de la entidad.

Un objetivo debe contar con las siguientes características:

Ilustración 5. Características de un objetivo.

S ***Specific* (específico):** Lo importante es resolver cuestiones como: qué, cuándo, cómo, dónde, con qué, quién. Considerar el orden y los necesarios para el cumplimiento de la misión.

M ***Mensurable* (medible):** Para ello es necesario involucrar algunos números en su definición, por ejemplo, porcentajes o cantidades exactas (cuando aplique).

A ***Achievable* (alcanzable);** Para hacer alcanzable un objetivo se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudará a saber si lo que se propone es posible o cómo resultaría mejor.

R ***Relevant* (relevante):** Considerar recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación.

T ***Timely* (temporal):** Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales.

Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025.

El proceso de identificación del riesgo es desarrollado por el responsable del proceso (Primera línea de defensa) y debe contar con el acompañamiento de la Oficina Asesora de Planeación (Segunda línea de defensa). En su desarrollo se deben responder las siguientes preguntas:

- ¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
- ¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto.
- ¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo con el desarrollo del proceso.
    - ¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo.

8.4.1 Clasificación del Riesgo por Factor

Para identificar adecuadamente los riesgos se recomienda que se lleve a cabo un análisis de matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas), esta es una técnica para ubicar los factores internos y externos identificados en la etapa previa y que afectan positiva o negativamente la forma en la cual una organización alcanza sus objetivos.

El ejercicio de la DOFA debe ser ejecutado en función de los objetivos estratégicos y los objetivos

del proceso. Como mínimo, este ejercicio se debe realizar una vez al año y debe ajustarse las veces que sea necesario.

El contexto estratégico de los procesos debe actualizarse como mínimo una vez en la vigencia y debe estar acorde con la caracterización y el objetivo definido para que los líderes de proceso o los enlaces MIPG en compañía de la Oficina Asesora de Planeación determinen la necesidad de incluir, ajustar, mantener y/o inactivar los riesgos de los procesos.

Esta actividad, debe realizarse en conjunto con la formulación de la planeación estratégica, confirmando los objetivos de los procesos establecidos. La Oficina Asesora de Planeación - OAP acompañará metodológicamente la construcción del contexto estratégico de los procesos, en este se determinan las Fortalezas, Debilidades, Oportunidades y Amenazas identificadas. Dicha información se representa en el formato DE-FR-004 Creación Actualización Contexto Estratégico FODA - V1 y se depositara en el repositorio que disponga la esta oficina.

Ilustración 6. Matriz DOFA.

Fuente: Elaboración Propia OAP

Las **debilidades** y **fortalezas** son de carácter interno y provienen del análisis del contexto o factor internos del proceso. De otro lado, las **oportunidades** y las **amenazas** corresponden al análisis del contexto o factor externo de la entidad y del proceso.

Tabla 3.Distribución DOFA.

DEBILIDADES	OPORTUNIDADES
Contexto interno	Contexto externo
FORTALEZAS	**AMENAZAS**
Contexto interno	Contexto externo

Fuente: Elaboración Propia OAP.

8.5 Identificación de áreas de impacto

Corresponde a la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que la entidad adopta son afectación económica (o presupuestal) y reputacional. Los cuales se evalúan para cada evento de riesgo identificado, pueden presentarse individualmente o en conjunto.

8.6 Identificación de áreas de factores de riesgo

Comprende las fuentes generadoras de riesgos, son las circunstancias o condiciones que aumentan la probabilidad de que ocurra el evento de riesgo, bien sea fuentes interna o externa. No son causas directas de los riesgos, pero incrementan el nivel de exposición.
A continuación, en la tabla 4. se establece el listado con los factores de riesgo que pueden incidir en los procesos.

Tabla 4.Factores de riesgo

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, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Falta de aplicación de los procedimientos
		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

Factor	Definición	Descriptores
		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 empleados que afectan la Integridad Pública.	Fraude Interno
		Soborno entrante
		Soborno saliente
		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
		Caída de redes
		Errores en hardware o software
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.	Fraude Externo
		Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

Los anteriores se deben relacionar con el desarrollo de los eventos proyectados en la Planeación Estrategia, el análisis de los factores y los elementos formulados que se aborden con la Dirección de la entidad.

8.7 Estructura de la descripción del Riesgo

Identificado lo anterior, se debe establecer la descripción del Riesgo la cual consta de la siguiente estructura impacto, causa inmediata y la causa raíz, de acuerdo con lo siguiente:

- **Impacto:** las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la entidad 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.
- **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. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Ilustración 7. Estructura del Riesgo.

Fuente: Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

Estos dos primeros 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. Debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar.

El último elemento identifica la causa raíz y condiciones contribuyentes que pueden clasificarse en: humanas, tecnológicas, normativas, ambientales, organizacionales. 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.

Ilustración 8. Ejemplo descripción de riesgo.

Ejemplo: posibilidad de afectactación económica y reputacional por incumplimientos a la gestión documental, debido a la pérdida de expedientes del archivo central.

En este caso se trata de un riesgo asociado a la gestión documental, pero esta causa raíz relacionada con la pérdida de expedientes puede representar un riesgo frente a la gestión contractual, la gestión jurídica y en cada proceso sus responsables y controles son específicos.

Fuente: Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

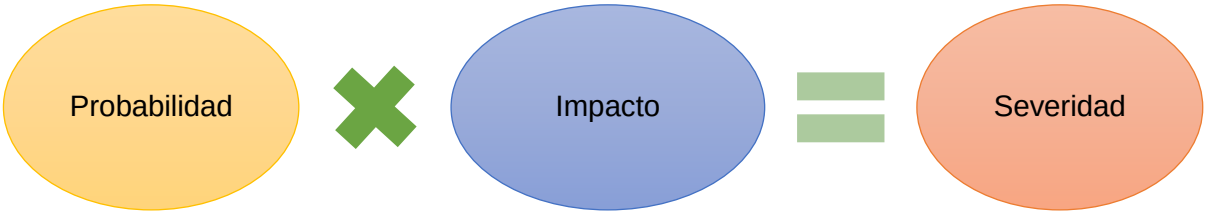
La descripción de los riesgos debe cumplir con lo siguiente:

- Los riesgos no se deben describir como fallas ni desviaciones de los controles.
- Evitar describir riesgos como la negación del control.
- No existen riesgos transversales, lo que puede existir son causas transversales.

8.7.1 Análisis De Riesgo Inherente

En esta etapa se determina el Riesgo Inherente (sin ningún tipo de aplicación de controles), a partir de la combinación de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, estableciendo el nivel de severidad.

Ilustración 9. Severidad del riesgo.



Fuente: Elaboración propia

Para tal fin, se utilizan los criterios establecidos en las siguientes tablas para medir el nivel de probabilidad y el impacto:

Tabla 5. Determinación de la probabilidad

	Frecuencia de la actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 1 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 2 a 1.000 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 1.001 a 5.000 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 5.001 veces al año y máximo 10.000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 10.001 veces por año	100%

Fuente: Adaptado Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

Se entiende como probabilidad a la posibilidad de ocurrencia del riesgo, en tal sentido estará asociada a la exposición al riesgo de la actividad que se esté analizando. De este modo, la probabilidad es el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Ejemplo: Para determinar la frecuencia con la cual se realiza esta actividad para el ejemplo planteado de “publicación de los planes, programas o proyectos”, se analiza la cantidad de veces que se realiza la publicación, suponiendo que se deban publicar 8 documentos 4 veces al año, se debe registrar la cantidad de veces que se presenta la posibilidad de materialización lo cual corresponde a 8 publicaciones x 4 veces al año = 32 publicaciones al año. Este valor será el que se registre en la matriz de riesgos.

Tabla 6. Determinación del impacto

	Afectación Económica	**Probabilidad**
Leve 20%	Afectación menor a 199 SMLMV	El riesgo afecta la imagen de algún área de la organización
Menor 40%	Entre 200 y 499 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y acciones y/o de proveedores
Moderado 60%	Entre 500 y 999 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 1.000 y 4.999 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 5.000 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Adaptado Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

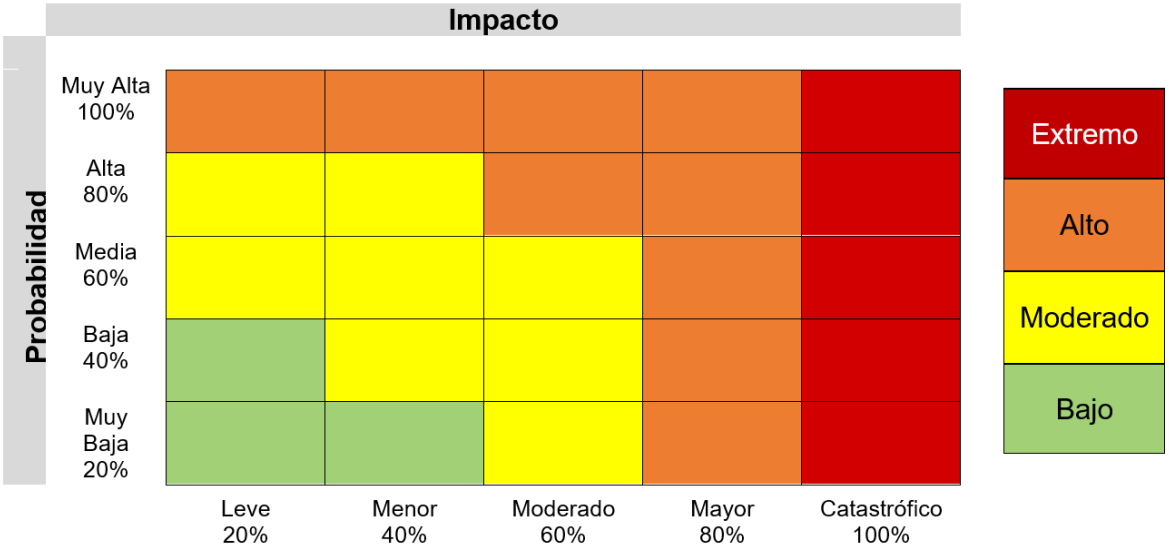
El impacto está asociado a las consecuencias que puede ocasionar el riesgo a la entidad por la materialización de un riesgo. Se asumen criterios de impacto económico y/o reputacional como las variables a evaluar. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel mayor e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel mayor.

8.7.2 Zonas de severidad

La entidad utiliza un mapa de calor para todas las tipologías de riesgo, el cual presenta 4 zonas de severidad según la probabilidad de ocurrencia y el impacto que podría generar cada riesgo. Este proceso consiste en evaluar qué tan probable es que el riesgo se materialice y qué consecuencias traería si esto sucede. Al ubicar el punto donde se cruzan estos dos factores en el mapa de calor, se determina el nivel de riesgo inherente de forma visual y práctica. Esta

representación gráfica facilita la toma de decisiones, ya sea para analizar un riesgo individual o para tener una visión integral de todos los riesgos identificados en el proceso y en la entidad.

Ilustración 10. Mapa de calor de Severidad



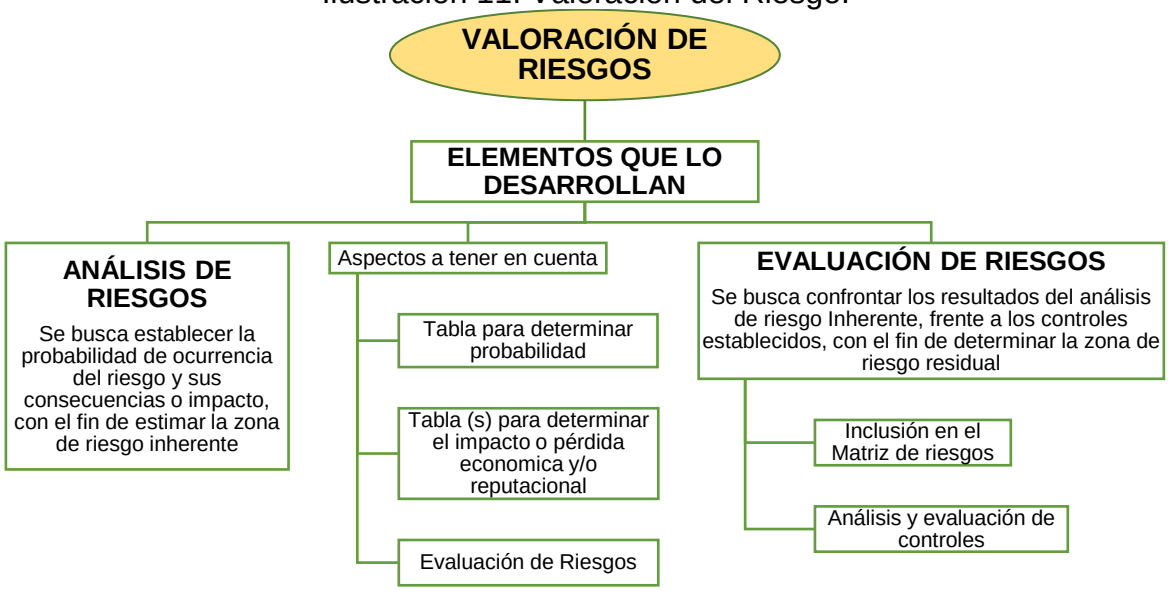
Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

8.8 Diseño, Análisis y Valoración de Controles

al determinar la probabilidad de ocurrencia y el nivel de consecuencia o impacto del riesgo para la entidad, como resultado se obtiene la zona de riesgo inherente, posteriormente los eventos son confrontados con la formulación de controles que permitan afrontar las causas detectadas permitiendo efectuar tratamiento y representar como resultado la zona de riesgo residual.

El escenario de valoración del riesgo se refleja de la siguiente manera:

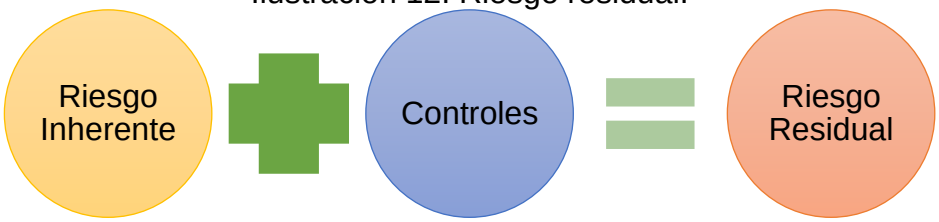
Ilustración 11. Valoración del Riesgo.



Fuente: Elaboración Propia

Luego de establecer el nivel de riesgo inherente se requiere la formulación de acciones concretas con atributos específicos con el propósito razonable que permita mitigar la posible materialización del riesgo detectado y por ende posible incumplimiento de los objetivos trazados. Esta etapa tiene como propósito tomar como punto de partida el nivel de Riesgo Inherente y como producto de la aplicación de controles establecer el nivel de Riesgo Residual.

Ilustración 12. Riesgo residual.



Fuente: Elaboración propia OAP

8.8.1 Diseño de controles

Los controles se pueden formular por medio de varios mecanismos, bien sea a través de las entrevistas con los líderes de procesos o los enlaces MIPG o los servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos, formatos que el proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo. Se recomienda que los controles a incluir en las matrices de riesgos se encuentren dentro de algún documento del sistema de gestión de la entidad.

Las actividades de control deben atender las causas raíz y enfocarse en la gestión de los factores de riesgo. Para ser efectivas deben contar con todos los atributos descritos en el presente numeral y cuando estén directamente relacionadas con las causas y factores de riesgo.

Para determinar la efectividad del control se debe tener en cuenta:

a. Estructura para la descripción del control

Responsable: Determina el cargo del responsable que ejecuta el control, se debe considerar la denominación del rol (Superintendente delegado, Jefe de oficina, Director, Coordinador, asesor, profesional, técnico, asistencial, profesional contratista designado). Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.

Se debe considerar que el responsable definido cuenta con el nivel de autoridad apropiado de cara a la actividad de control, así como aspectos básicos de segregación de funciones para evitar que quién sea la fuente generadora de riesgo, sea el único que aplica alguna actividad de control.

Objetivo del control: Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control. Ejemplos (Verificar, validar, conciliar, comparar, revisar, cotejar, detectar)

Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del control.

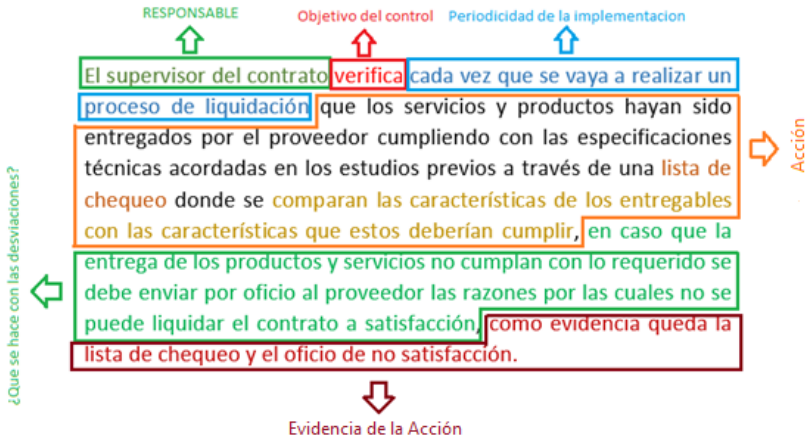
- Frecuencia (periodicidad de la implementación): Corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para prevenir, detectar o corregir el

posible evento de riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).

- Ejecución (Acción): Permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de presentarse desviaciones o situaciones que impidan su desarrollo. Puede darse a través de la comparación con información interna, externa o mixta. Se recomienda que su definición esté registrada en el sistema de gestión de la entidad (procedimientos, guías, instructivos, manuales, políticas, etc)
- Evidencia documentada (evidencia de la acción): Se refiere a la fuente documental que permite evidenciar la ejecución de los controles, bien sea formatos, base de datos, lista de chequeo, un acta de reunión, etc. Puede ser registro físico, manual o electrónico.

La siguiente es la estructura del control recomendada:

Ilustración 13. Estructura del control.



Fuente: Elaboración propia OAP

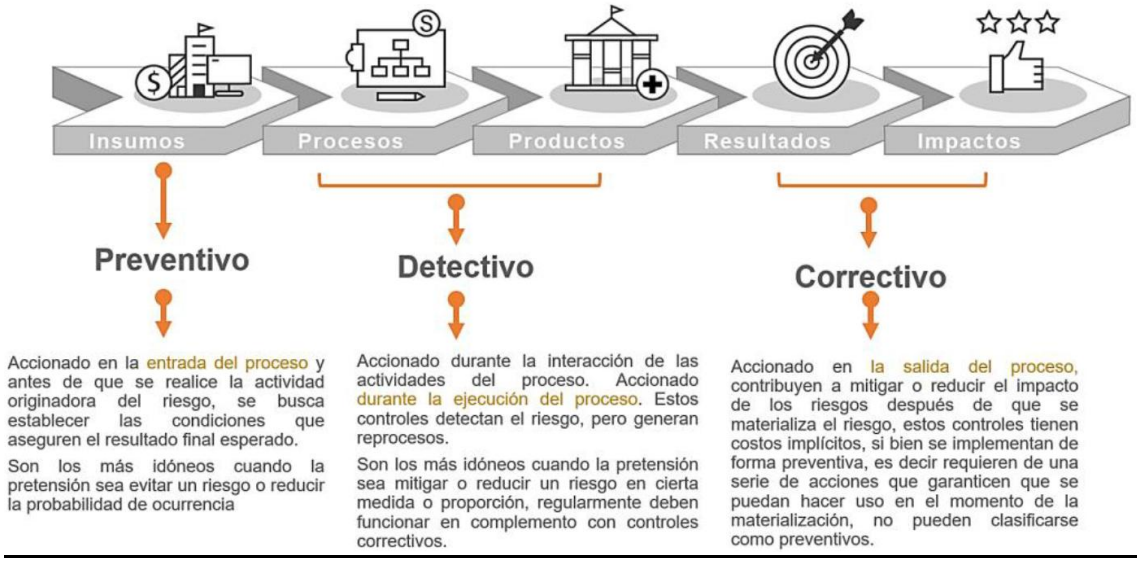
Tipología de controles

Control Preventivo: Control accionado en la entrada del proceso y antes que se realice la actividad originadora del riesgo, se busca establecer condiciones que aseguren el resultado final esperado

Control Detectivo: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo durante la ejecución del proceso y puede disminuir la materialización de dicho riesgo, pero generar reprocesos.

Control Correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Ejemplos: pólizas de seguro, copias de seguridad (backup), bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez materializado.

Ilustración 14. Tipologías de control.



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- Control manual: ejecutados por personas.
- Control automático: ejecutados por un sistema o software previamente programado o diseñado.

b. Análisis y evaluación de los controles

Teniendo en cuenta las características propias del control se realiza su evaluación, a través de estos atributos:

Tabla 7. Atributos del control.

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%
***Atributos Informativos**	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).		-
	Evidenci	Con registro manual	Se deja evidencia o rastro de la ejecución del control.	-
		Con registro electrónico		-
	E	Interna	Formatos o registros internos formales.	=

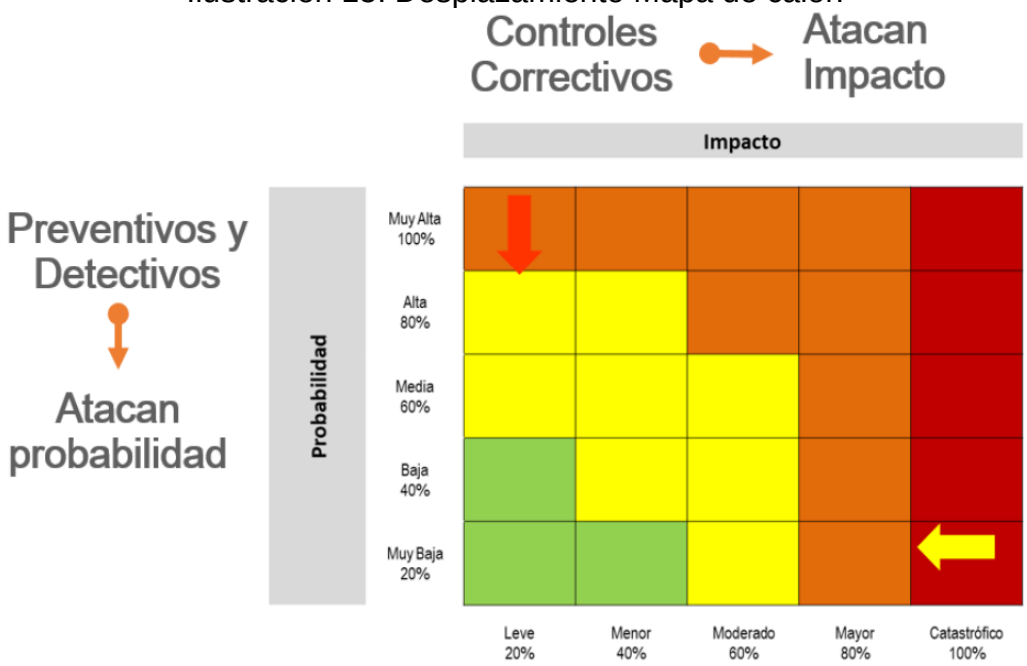
		Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).	=
		Mixta	Combinación de datos de fuentes internas y externas formales.	=

Fuente: Elaboración propia.

Aplicación de controles y riesgo residual

A partir de la aplicación de controles se obtiene el movimiento o desplazamiento del nivel de riesgo inherente en la matriz de calor, a continuación, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Ilustración 15. Desplazamiento Mapa de calor.



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

El Riesgo Residual corresponde al estado real del riesgo, luego de la valoración del riesgo inherente y la aplicación de los controles; lo que conlleva a identificar la necesidad de implementación de controles o mejoras adicionales sobre los existentes.

La fórmula dada para valorar los controles que afecten la probabilidad equivale a la resta de la valoración dada a la probabilidad de ocurrencia del riesgo menos el resultado de multiplicar la valoración dada a la probabilidad de ocurrencia del riesgo por el valor del control.

PI= Probabilidad Inherente
PR= Probabilidad Residual
VC= Valoración del Control

PR = PI – (PI * VC)

Como puede existir más de un control para mitigar la misma probabilidad de ocurrencia de un riesgo, para el segundo control se tomará PR como PI.

PR1 = PI – (PI * VC1)
PR2 = PR1 – (PR1 * VC2)
PR3 = PR2 – (PR2 * VC3)
PRn = PRn-1 – (PRn-1 * VCn)

Lo mismo ocurre para la valoración de los controles que afecten el impacto siendo la fórmula resultante la que se muestra a continuación:

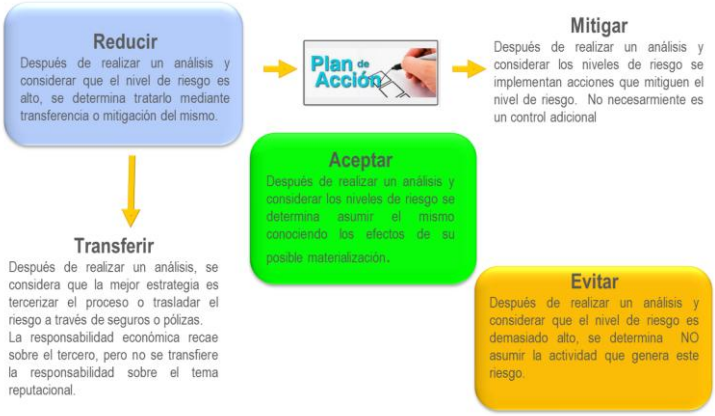
II= Probabilidad Inherente
IR= Probabilidad Residual
VC= Valoración del Control

IR1 = II – (II * VC1)
IR2 = IR1 – (IR1 * VC2)
IR3 = IR2 – (IR2 * VC3)
IRn = IRn-1 – (IRn-1 * VCn)

8.9 Tratamiento del Riesgo

Esta etapa se busca establecer las acciones que se aplicarán a los riesgos identificados luego de la obtención del riesgo residual considerando aplicar las opciones de tratamiento de acuerdo con el nivel de riesgo obtenido y desarrollar planes en caso de ser necesario.
A continuación, se describen las opciones para el tratamiento del riesgo:

Ilustración 16. Tratamiento del Riesgo.



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

- Reducir: luego de los resultados obtenidos se determina mediante transferencia o mitigación, en ambos casos corresponde a la Implementar controles para reducir la probabilidad o el impacto.
  - Transferir: Compartir las consecuencias de la materialización del riesgo, por ejemplo, a través de la adquisición de una póliza.
  - Mitigar: Acciones adicionales que mitiguen el nivel de riesgo.
- Aceptar: Cuando el nivel del riesgo está por debajo del apetito establecido por la alta dirección.
- Evitar: Cuando se decide evitar la realización de la actividad que representa el riesgo.

Verificar para cada tipología de riesgo el tratamiento en el desarrollo de su capítulo.

8.10 Consolidación en el mapa de riesgos.

Para crear, modificar o desactivar riesgos o controles, es necesario contar con un acta de reunión firmada por el Líder del proceso o Enlace MIPG junto con la jefatura de la Oficina Asesora de Planeación o el profesional designado para la Gestión Integral de Riesgos. Una vez firmada el acta, se procederá a incluir y consolidar los cambios en el Mapa Institucional de Riesgos.
Es importante tener en cuenta que no se pueden realizar ajustes al mapa sin contar con el acta de reunión debidamente firmada. Los riesgos y controles que se consideran vigentes son aquellos publicados en la versión más reciente del Mapa Institucional de Riesgos disponible en la página web de la entidad.

8.10.1 Inactivación de un riesgo.

Sí dentro de este ejercicio, el líder de proceso u operativo identifica la necesidad de inactivar un riesgo y por ello debe retirarse de la matriz de riesgos, notificará a la Oficina Asesora de Planeación la necesidad de excluirlo siempre y cuando no existan recomendaciones u observaciones respecto a la ejecución de controles o al riesgo en sí mismo en los informes de auditoría, evaluación o de seguimiento a riesgos, si se identifican se deberá mantener en la matriz.

La notificación debe contener la justificación técnica y detallada de la inactivación del riesgo del proceso, la cual será presentada por el líder operativo responsable. Este hecho quedará debidamente registrado en el informe de seguimiento elaborado por la segunda línea de defensa, garantizando la trazabilidad de la decisión adoptada del proceso

9. TIPOLOGÍAS DE RIESGO

La entidad asume la gestión integral de riesgos y mediante la presente política gestiona las siguientes tipologías: Gestión, Seguridad de la Información, Fiscales y Riesgos para la Integridad Pública.

Sin embargo, el presente lineamiento permite la articulación y vinculación con las Políticas y entornos de seguimiento establecidos para el ejercicio e implementación del Modelo Integrado de Planeación y Gestión - MIPG.

9.1 Riesgos de Gestión.

Corresponde a los riesgos asociados a la operación de la entidad, al ser propios o intrínsecos a las procesos, funciones y misionalidad de cada entidad. Los riesgos de gestión son aquellos posibles efectos que se causan sobre los objetivos de la entidad, debido a eventos potenciales, que hacen referencia a la posibilidad de incurrir en pérdidas económicas o reputacionales por deficiencias, fallas o inadecuaciones, en la “ejecución y administración de procesos”, “tecnología” e “infraestructura”, generados por falencias en la operación.

Por lo anterior la selección de los siguientes factores determina la clasificación del evento de riesgo en la tipología de Gestión:

Tabla 8. Factores de riesgos de Gestión.

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, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Falta de aplicación de los procedimientos
		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
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de sistemas de información y aplicaciones
		Caída de redes
		Errores en hardware o software
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

Para esta tipología de riesgos se desarrollan los siguientes numerales del presente lineamiento sin modificación:

8.7 Estructura de la descripción del Riesgo

8.8 Diseño, Análisis y Valoración de Controles
8.9 Tratamiento del Riesgo
8.10 Consolidación en el Mapa de Riesgos

9.1.1 Monitoreo y seguimiento.

El monitoreo y seguimiento se realiza acorde con lo definido en el numeral "*6 Responsabilidades*" del presente documento (Responsabilidades), en el cual se detalla lo establecido en la dimensión 7ª (Control Interno) del Modelo Integrado de Planeación y Gestión (MIPG) y a la aplicación de las líneas de defensa para identificar la responsabilidad de la gestión del riesgo. La periodicidad para el seguimiento de los riesgos, los controles y el plan de acción se realiza acorde con lo descrito en la siguiente Tabla.

Tabla 9. Responsabilidades Riesgos de Gestión.

Responsable	Riesgos de Gestión
Primera línea de defensa (líderes de procesos, Enlaces MIPG)	• Implementar, ejecutar y monitorear los controles y el plan de acción (si aplica) propendiendo por su adecuado desarrollo y cumplimiento acorde a lo establecido en Mapa Institucional de Riesgos. • Gestionar y documentar de manera directa en el día a día los riesgos de su proceso o de las actividades en las que participa. <u>Cargue de Evidencias Trimestral:</u> A más tardar el 10° día hábil una vez terminado el trimestre, el líder de proceso o el enlace MIPG de cada uno de los procesos debe disponer las evidencias en el repositorio institucional destinado para tal fin por parte de la oficina Asesora de Planeación - OAP. A su vez debe registrar el seguimiento del comportamiento del control(es) en la herramienta indicada por la OAP
Segunda línea de defensa	<u>Periodicidad trimestral</u> Verificar y monitorear la ejecución de los controles y el plan de acción (si aplica) implementados por la primera línea de defensa para mitigar los riesgos. A más tardar el 15° día hábil una vez terminado el trimestre debe elaborar un informe con el monitoreo a los riesgos de los procesos retroalimentando al despacho del superintendente, a los líderes de los procesos y a la

Responsable	Riesgos de Gestión
	tercera línea de defensa sobre el comportamiento durante el periodo de seguimiento. Debe garantizar la custodia de las evidencias en el repositorio institucional administrado por la Oficina Asesora de Planeación. El informe debe publicarse en la Web de la Entidad para conocimiento de las partes interesadas.
Tercera línea de defensa	De acuerdo con el plan anual de auditoría aprobado por el CICCI. - Realiza seguimiento a través de la auditoría interna (auditoría, evaluación o seguimiento), mecanismo utilizado para evaluar integralmente con independencia y objetividad la efectividad del sistema de control interno, y la gestión de los riesgos llevada a cabo por la primera y segunda línea de defensa. - Las evidencias de los controles y del plan de acción deben consultarse en el repositorio establecido por la Oficina Asesora de Planeación.

Fuente: Elaboración propia.

Es necesario reiterar que la responsabilidad de la línea de defensa estratégica es supervisar el cumplimiento de la Política para la Gestión Integral de Riesgos y evaluar su eficacia en el marco del desarrollo del Comité Institucional de Coordinación de Control Interno - CICCI.

9.1.2 Materialización de riesgos.

Dado que en cualquier momento un riesgo puede materializarse, es fundamental contar con una orientación clara sobre cómo actuar cuando esto suceda. Cualquier línea de defensa puede reportar la materialización de un riesgo, ya sea identificado previamente o no.

A continuación, se describen las acciones que deben seguirse en caso de materialización.

Tabla 10. Acciones en caso de materialización.

TIPO DE RIESGO	ACCIONES
Riesgos de gestión	La línea de defensa que detecte la materialización debe informar a la segunda y tercera línea de defensa de la materialización del riesgo y generar alerta de las posibles consecuencias.
	El proceso responsable de la ejecución de la actividad debe hacer una

	descripción detallada de lo ocurrido y del impacto generado a los objetivos del proceso y de la Entidad por la materialización del riesgo.
	El proceso responsable de la ejecución de la actividad en conjunto con la Segunda línea de defensa debe revisar la identificación y valoración del riesgo, analizando las causas que lo generaron y los controles existentes con el fin de evitar que se materialice nuevamente el riesgo.
	El proceso responsable de la ejecución de la actividad basado en el diagnóstico de la situación presentada, establecer un plan de acción fundamentado en la actualización del mapa de riesgos.
	La segunda línea de defensa debe realizar seguimiento mensual para medir la efectividad de las acciones establecidas en el plan de acción.

Fuente: Elaboración Profesional Oficina Asesora de Planeación - OAP.

El resultado del ejercicio debe socializarse a la Línea Estratégica mediante el Comité Institucional de Control Interno – CICCI una vez culminado el periodo de seguimiento, las acciones antes descritas deben contar con el apoyo metodológico de la Oficina Asesora de Planeación.

9.1.3 Materialización de riesgos no identificados.

En el evento en que alguna de las líneas de defensa evidencien el incumplimiento de algún objetivo establecido por un proceso o la entidad que no se encuentre registrado en el Mapa de Riesgos Institucional con la posibilidad de generar pérdidas económicas o reputacionales a la entidad, se debe proceder con mesa de trabajo entre el proceso responsable y la Oficina Asesora de Planeación para continuar con la inclusión del evento en el Mapa de Riesgos Institucional cumpliendo con lo descrito en el presente Capitulo.

9.2 Riesgos de Seguridad de la Información.

Los lineamientos para la formulación e implementación de la Gestión de Riesgos de Seguridad de la Información que se puedan presentar en el desarrollo de la gestión de la entidad y están fundamentados en el Anexo 4. “Lineamientos para la Gestión de Riesgos de Seguridad Digital en entidades públicas” del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, ISO/IEC 27002:2022 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad — Controles de seguridad de la información y la “Guía para la Gestión Integral del Riesgo en Entidades Públicas” del Departamento Administrativo de la Función Pública - DAFP.

Los Riesgos de Seguridad Digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, Confidencialidad o Disponibilidad” que permiten cumplir con la misión y alcanzar la Visión de la entidad.

- **Integridad:** Se refiere a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros no autorizados.
- **Confidencialidad:** Se refiere a cómo los datos se mantienen al acceso únicamente de las personas o sistemas que se encuentran autorizados.
- **Disponibilidad**: Se refiere al acceso de la información en el momento que debe estar disponible; se aclara que la información de la entidad no debe estar disponible todo el tiempo durante el año.

En tal sentido, para la identificación de Riesgos de Seguridad de la Información es necesario en primera instancia identificar los activos de información de la entidad y los procesos, teniendo en cuenta los siguientes pasos:

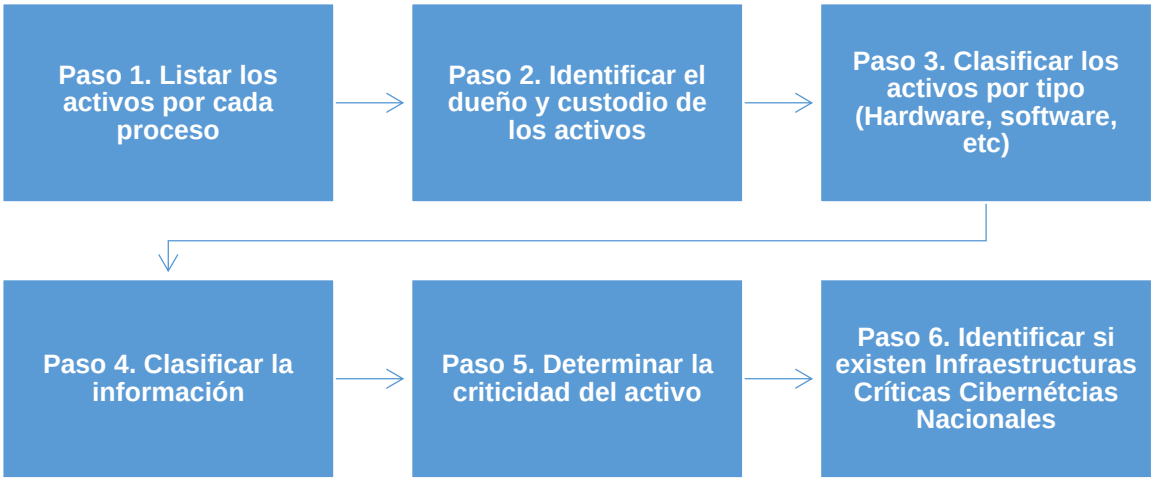
9.2.1 Identificación de los activos de seguridad de la información.

Para la Identificación de Riesgos de Seguridad de la Información es necesario contar con el inventario de activos de información por proceso aprobado y publicado. Es importante recordar que un activo de información es cualquier información que aporte valor a la entidad dentro de los cuales se pueden encontrar elementos (información, aplicaciones, hardware, personas, entre otros), que se deben proteger para garantizar el funcionamiento interno de cada proceso.

Los líderes de los procesos deben coordinar las actividades necesarias para realizar el levantamiento, actualización y clasificación de los activos de la información con el acompañamiento del Oficial de Seguridad y Privacidad de la Información. La clasificación de los activos deberá realizarse conforme a las categorías establecidas en el Modelo de Seguridad y Privacidad de la Información – MSPI (Resolución 2277 de 2025), identificando Activos Críticos, Altamente Críticos, Activos de Soporte y Activos asociados a Servicios Ciudadanos Digitales, con el fin de priorizar su protección dentro del proceso de gestión de riesgos.
De igual forma para la Gestión de los Riesgos de Seguridad Digital, los líderes de cada proceso deben definir los activos de información, clasificarlos e identificar si existen infraestructuras criticas cibernéticas, teniendo en cuenta las situaciones no deseadas, la pérdida de confidencialidad, integridad y disponibilidad de la información, así poder identificar los activos que requieren ser custodiados y protegidos que permitan garantizar el funcionamiento interno en la entidad, así como el funcionamiento de cara al ciudadano.

Los siguientes son los pasos para desarrollar para la identificación y valoración de activos.

Ilustración 17, Pasos para la identificación y valoración de activos



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

9.2.2 Identificación de Riesgos de Seguridad de la información.

La Gestión de los Riesgos de Seguridad Digital y Privacidad de la Información se ejerce en integración con el MSPI (Modelo de Seguridad y Privacidad de la Información) y con el MGRSD (Modelo de Gestión de Riesgos de Seguridad de la Información) determinado por MINTIC. Así mismo, en la determinación de las fases para la Gestión de Riesgos, se incluyen las ICC (Infraestructuras Críticas Cibernéticas) como parte de los activos de la información. En la identificación y valoración de riesgos se deberán considerar las amenazas, vulnerabilidades y controles definidos en el Catálogo de Controles del MSPI (Resolución 2277 de 2025), incluyendo riesgos asociados a ciberseguridad, infraestructura tecnológica, redes, aplicaciones, servicios en la nube y contratos con proveedores de tecnología y licencias.

Las afectaciones que pueden generar daño a un activo o un grupo de activos inherentes a la seguridad de la información son:

- Pérdida de confidencialidad de la información.
- Pérdida de la integridad de la información.
- Pérdida de la disponibilidad de la información.

Dentro de las amenazas podemos identificar amenazas comunes como son, aquellas que causan daño a la infraestructura tecnológica, a los servicios, al cumplimiento de las funciones y comprometiendo así los activos. Pueden ser Deliberadas (D), fortuitas (F) o ambientales (A). la siguiente es la relación de amenazas comunes:

Tabla 11. 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
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

Tipo	Amenaza	Origen
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.

Del mismo modo se cuenta con la relación de las vulnerabilidades comunes:

Tabla 12. Tabla de Vulnerabilidades Comunes.

Tipo	Vulnerabilidades
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)
	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

Tipo	Vulnerabilidades
	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

Tipo	Vulnerabilidades
	limpia entre otros)

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

Los lineamientos se encuentran detallados en el "*Manual de Gestión de Riesgos de Seguridad código TIC-MA-007*". El cual tiene como objetivo establecer las directrices para la gestión del riesgo de seguridad de la información para la Superintendencia de Transporte, esto se logra a través de la identificación, análisis, valoración y tratamiento de los riesgos relacionados con los objetivos de los procesos, con el fin de facilitar su cumplimiento, así como los objetivos estratégicos de la organización.

En dicho manual, en el apartado titulado "*5.2 IDENTIFICACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN*", se describe la metodología para identificar y redactar los riesgos de seguridad de la información.

Para esta tipología de riesgos se desarrollan los siguientes numerales del presente lineamiento sin modificación:

8.7 Estructura de la descripción del Riesgo
8.8 Diseño, Análisis y Valoración de Controles
8.9 Tratamiento del Riesgo

9.2.3 Consolidación en el Mapa de Riesgos

Dada su especificidad y tratamiento los riesgos de Seguridad de la información se consolidan individualmente en la matriz de riesgos de seguridad de la información. Aplica lo descrito en el numeral 9.11.1. Inactivación de un riesgo.

9.2.4 Monitoreo y seguimiento.

El monitoreo y seguimiento de los Riesgos de Seguridad de la Información se lleva a cabo de acuerdo con lo establecido en el numeral "6. Responsabilidades", que detalla lo establecido en la dimensión 7ª (Control Interno) del Modelo Integrado de Planeación y Gestión (MIPG), así como la aplicación de las líneas de defensa para identificar la responsabilidad en la gestión del riesgo. La periodicidad para el seguimiento de los riesgos, los controles y el Plan de Acción se realiza conforme a lo indicado en la tabla que se presenta a continuación. Es necesario reiterar que la responsabilidad de la línea de defensa estratégica es supervisar el cumplimiento de la Política para la Gestión Integral de Riesgos y evaluar su eficacia en el contexto del desarrollo del Comité

Institucional de Coordinación de Control Interno – CICCI o quien se defina para tal fin.

Tabla 13. Responsabilidades Riesgos de Seguridad de la información.

Responsable	Riesgos de Seguridad de la información
Primera línea de defensa (líderes de procesos, Enlaces MIPG)	• Implementar, ejecutar y monitorear los controles y el plan de acción (si aplica), propendiendo por su adecuado desarrollo y cumplimiento acorde a lo establecido en la matriz de Riesgos. • Gestionar y documentar de manera directa en el día a día los riesgos de su proceso o de las actividades en las que participa. <u>Cargue de Evidencias Cuatrimestral:</u> A más tardar el 10° día hábil una vez terminado el trimestre el líder de proceso o Enlace MIPG de cada uno de los procesos debe disponer las evidencias en el repositorio institucional destinado para tal fin por parte de la oficina Asesora de Planeación - OAP. A su vez debe registrar el seguimiento del comportamiento del control(es) en la herramienta indicada por la OAP
Segunda línea de defensa (Oficina de Tecnologías de la Información y las Comunicaciones)	<u>Periodicidad Cuatrimestral</u> Verificar y monitorear la ejecución de los controles y el plan de acción implementados por la primera línea de defensa para mitigar los riesgos. A más tardar el 15° día hábil una vez terminado el cuatrimestre debe elaborar un informe con el monitoreo y seguimiento a los riesgos de los procesos retroalimentando al líder de proceso e informando a la tercera línea de defensa sobre el comportamiento durante el periodo de seguimiento. Debe garantizar la custodia de las evidencias en el repositorio institucional administrado por la Oficina Asesora de Planeación. El informe debe publicarse en la Web de la Entidad para conocimiento de las partes interesadas.
Tercera línea de defensa	<u>De acuerdo con el plan anual de auditoría aprobado</u> - Realiza seguimiento a través de la auditoría interna, mecanismo utilizado para evaluar

Responsable	Riesgos de Seguridad de la información
	integralmente con independencia y objetividad la efectividad del sistema de control interno y la gestión de los riesgos llevada a cabo por la primera y segunda línea de defensa. - Las evidencias de los controles y del plan de acción deben consultarse en el repositorio establecido por la Oficina Asesora de Planeación

Fuente: Elaboración propia. Basado en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6, 2022

El resultado del ejercicio debe socializarse por la segunda línea de defensa (OAP) a la Línea de defensa Estratégica mediante el Comité Institucional de Control Interno – CICCI una vez culminadas las actividades mencionadas para la tercera línea de defensa.

9.2.5 Materialización de riesgos.

Dado que en cualquier momento un riesgo puede materializarse, es fundamental contar con una orientación clara sobre cómo actuar cuando esto suceda. A continuación, se describen las acciones que debe seguir la Primera línea de defensa en caso de materialización.

Tabla 14. Acciones en caso de materialización.

TIPO DE RIESGO	ACCIONES
Riesgos de Seguridad de la Información	Informar a la segunda y tercera línea de defensa de la materialización del riesgo y generar alerta de las posibles consecuencias.
	Hacer una descripción detallada de lo ocurrido y del impacto generado a los objetivos del proceso y de la Entidad por la materialización del riesgo.
	Revisar la identificación y valoración del riesgo, analizando las causas que lo generaron y los controles existentes con el fin de evitar que se materialice nuevamente el riesgo.
	Basados en el diagnóstico de la situación presentada, establecer un plan de acción fundamentado en la actualización del mapa de riesgos.
	Realizar seguimiento mensual para medir la efectividad de las acciones establecidas en el plan de acción.

Fuente: Elaboración Profesional Oficina Asesora de Planeación.

El resultado del ejercicio debe socializarse a la Línea de defensa Estratégica mediante el Comité Institucional de Control Interno - CICCI, las acciones antes descritas deben contar con el apoyo

metodológico de la OAP y la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

9.3 Riesgos Fiscales

Corresponde al análisis de la operación de la entidad para identificar y gestionar los riesgos que puedan provocar un daño patrimonial, 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.

Las bases del ámbito normativo y jurídico del control fiscales están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, modificadas por el Acto Legislativo 04 de 2019 fundamentado en la necesidad de un ejercicio preventivo del control fiscal, que detenga el daño fiscal e identifique los riesgos fiscales en la entidad; con ello, la línea estratégica podrá adoptar las medidas necesarias para prevenir la concreción del daño patrimonial de naturaleza pública.

El Riesgo Fiscal se define como el “Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial”, el cual surge de los daños que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, si bien La Ley 610 de 2000 establece el trámite de los procesos de responsabilidad fiscal es de competencia de las contralorías, se evidencia que el control fiscal efectuado por dichas entidades además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante con carácter excepcional, no vinculante, no implica coadministración, no versa sobre la conveniencia de las decisiones de los administradores de recursos públicos, se realiza en forma de advertencia al gestor fiscal y deberá estar incluido en un sistema general de advertencia público; se busca generar el desarrollo preventivo al interior de la entidad con el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, protegiendo la entidad de la perdida de recursos públicos, bienes o intereses patrimoniales a cargo de los gestores fiscales (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros), lo cual contribuye al cumplimiento de sus funciones y al aseguramiento razonable para la toma de decisiones.

9.3.1 Identificación de áreas de factores de riesgo

Las fuentes generadoras de riesgos para esta tipología aplican todos los factores relacionados en la tabla 4 debido a que todas las circunstancias o condiciones pueden aumentar la probabilidad de que ocurra el evento de riesgo fiscal.

9.3.2 Identificación del Riesgo

Para la identificación del Riesgo Fiscal es necesario seguir los siguientes pasos:

Ilustración 18. Pasos para la identificación del riesgo fiscal

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

Para establecer los **puntos de Riesgo Fiscal** que corresponde a las actividades en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas, se toman como punto de partida aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal en la entidad.

Complementando el ejercicio de los puntos de riesgo se deben identificar las **circunstancias inmediatas**, siendo aquellas situaciones o actividades bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o causa raíz para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas. Para mantener unificado el criterio de identificación del riesgo la **Circunstancia Inmediata** corresponde a la **Causa Inmediata** definida para los Riesgos de Gestión.

9.3.3 Identificación de Puntos de Riesgo Fiscales y Causa Inmediata

Como complemento a la identificación del riesgo se debe adelantar el siguiente cuestionario:

- **Cuestionario de Identificación:** Se debe efectuar con los líderes de procesos u operativos, en compañía de los asesores y servidores que se consideren necesarios por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de gestión fiscal en las que potencialmente se genera riesgo fiscal) y causas inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal).

    - ¿En qué procesos de la entidad se realiza Gestión Fiscal?
    - ¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo 1[2]), son aplicables a la entidad?
    - ¿Cuáles son los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal relacionados con hechos de la entidad y las advertencias recibidas por Contraloría de Bogotá o la OCI?
    - ¿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?

Los ejercicios antes descritos deben efectuarse como mínimo una vez al año y deben respaldarse con actas de reunión con los líderes de proceso u operativos. El ejercicio se respalda con la verificación de Matriz de Plan de Mejoramiento de Contraloría de la entidad y la asesoría de la OCI.

9.3.4 Identificación de áreas de impacto

Para el contexto del riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse esta tipología de riesgo.

---

[2] Este catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias Inmediatas, es el resultado del análisis de investigaciones previas y del estudio detallado de información sobre:

(i) Fallos con responsabilidad fiscal, en firme, emitidos en los últimos 3 años, por una muestra de 10 de las contralorías territoriales mejor calificadas en 2020, según el criterio de desempeño integral, el cual corresponde a evaluación realizada por la Auditoría General de la República.

(ii) Muestra aleatoria de fallos con responsabilidad fiscal, en firme, emitidos por la Contraloría General de la República en los últimos 3 años.

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

Tabla 15. Pasos para la identificación del riesgo fiscal

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

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

9.3.5 Identificar el efecto económico

Es importante precisar que el efecto económico del riesgo fiscal es determinado como el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público. De la misma manera es importante indicar 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.

Lo siguientes son ejemplos de efectos económicos que no son riesgos fiscales:
(i) Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.
(ii) Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público
(iii) Multas impuestas por hechos que no comportan gestión fiscal
(iv) Existencia de actuación de cobro coactivo por parte de la entidad.

(v) 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.
(vi) 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).

9.3.6 Identificación de la causa raíz o potencial hecho generador

La causa raíz o potencial hecho generador es aquel evento potencial (acción u omisión) que provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño/Impacto) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio.

Para mantener la adecuada Gestión del Riesgo se exige que la identificación de causas sea objetiva y rigurosa, permitiendo ya que los controles que se diseñen e implementen apunten a atacar las causas, para así lograr prevenir la ocurrencia de daños fiscales.

9.3.7 Descripción del Riesgo Fiscal

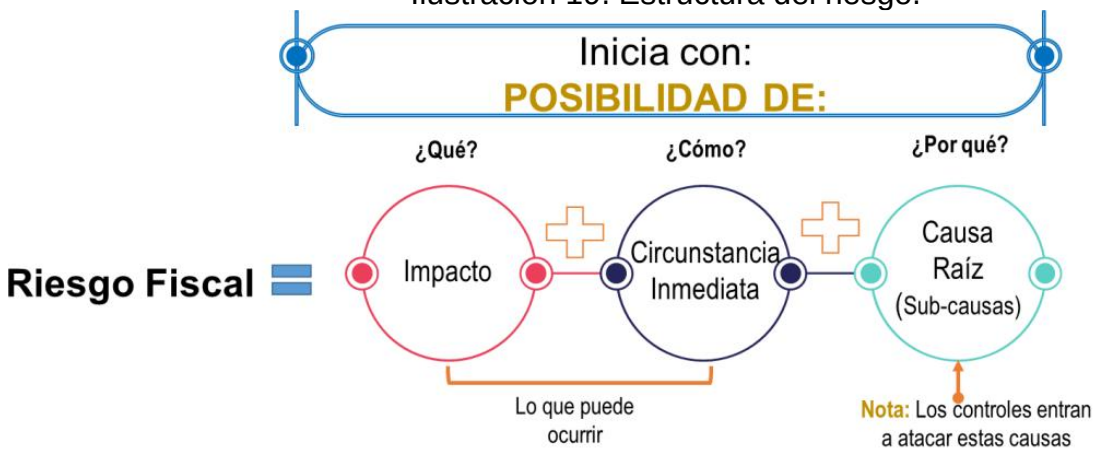
Para lograr diferenciar los riesgos fiscales de las demás tipologías se debe formular y redactar adecuadamente permitiendo su entendimiento y tratamiento pertinente.

Para redactar un Riesgo Fiscal se debe tener en cuenta:
✓ Iniciar con la expresión **Posibilidad de**, debido a que nos estamos refiriendo al evento potencial.
✓ Impacto: Corresponde al **qué**. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza
✓ Causa (Circunstancia) inmediata: Corresponde al **cómo**. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

✓ Causa Raíz: Corresponde al **por qué**; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:

Ilustración 19. Estructura del riesgo.



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

La descripción del riesgo debe contener todos los detalles antes ilustrados con la intención de que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. La estructura facilita su redacción y claridad, evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

A continuación, la estructura de redacción de un riesgo fiscal dando atención a lo manifestado:

Ilustración 20. Estructura del Riesgo Fiscal.

Fuente: Elaboración Propia

Otros ejemplos de Riesgos Fiscales son:

Tabla 16. Ejemplos de Riesgo Fiscal.

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la implementación y operación de redes eléctricas seguras.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la ejecución de proyectos de infraestructura sin la aprobación de licencias ambientales requeridas.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por negación del reconocimiento de siniestros en el contrato de seguro, a causa de la omisión en la actualización del inventario de bienes amparados.

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por pérdida, extravío o hurto de bienes muebles de la entidad a causa de la inexistencia de procedimientos documentados para el ingreso y salida de bienes del almacén	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por menores ingresos percibidos sobre la explotación de marcas de propiedad comercial de la entidad a causa de errores u omisiones en el análisis técnico, jurídico y económico del mercado
Posibilidad de efecto dañoso sobre bienes públicos, por deterioro de la infraestructura a causa de la realización de la programación de mantenimientos preventivos y correctivos	Posibilidad de efecto dañoso sobre los recursos de la entidad por la generación de intereses moratorios en contrato de arrendamiento a causa de la omisión en el pago oportuno del canon pactado.	Posibilidad de efecto dañoso sobre los intereses patrimoniales por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora a causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

Para esta tipología de riesgos se desarrollan los siguientes numerales del presente lineamiento sin modificación:

8.7 Estructura de la descripción del Riesgo
8.8 Diseño, Análisis y Valoración de Controles
8.9 Tratamiento del Riesgo
8.10 Consolidación en el Mapa de Riesgos

9.3.8 Monitoreo y seguimiento.

El monitoreo y seguimiento se realiza acorde con lo definido en el numeral "*6 Responsabilidades*" del presente documento (Responsabilidades), en el cual se detalla lo establecido en la dimensión 7ª (Control Interno) del Modelo Integrado de Planeación y Gestión (MIPG) y a la aplicación de las líneas de defensa para identificar la responsabilidad de la gestión del riesgo. La periodicidad para el seguimiento de los riesgos, los controles y el plan de acción se realiza acorde con lo descrito en la siguiente Tabla.

Tabla 17. Responsabilidades Riesgos Fiscales.

Responsable	Riesgos Fiscales
Primera línea de defensa (líderes de procesos, Enlaces MIPG)	• Implementar, ejecutar y monitorear los controles y el plan de acción (si aplica) propendiendo por su adecuado desarrollo y cumplimiento acorde a lo establecido en Mapa Institucional de Riesgos. • Gestionar y documentar de manera directa en el día a día los riesgos de su proceso o de las actividades en las que participa. <u>Cargue de Evidencias Trimestral:</u> A más tardar el 10° día hábil una vez terminado el trimestre, el líder de proceso o el enlace MIPG de cada uno de los procesos debe disponer las evidencias en el repositorio institucional destinado para tal fin por parte de la oficina Asesora de Planeación - OAP. A su vez debe registrar el seguimiento del comportamiento del control(es) en la herramienta indicada por la OAP
Segunda línea de defensa	<u>Periodicidad trimestral</u> Verificar y monitorear la ejecución de los controles y el plan de acción (si aplica) implementados por la primera línea de defensa para mitigar los riesgos. A más tardar el 15° día hábil una vez terminado el trimestre debe elaborar un informe con el monitoreo a los riesgos de los procesos retroalimentando al despacho del superintendente, a los líderes de los procesos y a la tercera línea de defensa sobre el comportamiento durante el periodo de seguimiento. Debe garantizar la custodia de las evidencias en el repositorio institucional administrado por la Oficina Asesora de Planeación. El informe debe publicarse en la Web de la Entidad para conocimiento de las partes interesadas.

Responsable	Riesgos Fiscales
Tercera línea de defensa	De acuerdo con el plan anual de auditoría aprobado por el CICCI. - Realiza seguimiento a través de la auditoría interna (auditoría, evaluación o seguimiento), mecanismo utilizado para evaluar integralmente con independencia y objetividad la efectividad del sistema de control interno, y la gestión de los riesgos llevada a cabo por la primera y segunda línea de defensa. - Las evidencias de los controles y del plan de acción deben consultarse en el repositorio establecido por la Oficina Asesora de Planeación.

Fuente: Elaboración propia.

Es necesario reiterar que la responsabilidad de la línea de defensa estratégica es supervisar el cumplimiento de la Política para la Gestión Integral de Riesgos y evaluar su eficacia en el marco del desarrollo del Comité Institucional de Coordinación de Control Interno - CICCI.

9.3.9 Materialización de riesgos.

Dado que en cualquier momento un riesgo puede materializarse, es fundamental contar con una orientación clara sobre cómo actuar cuando esto suceda. A continuación, se describen las acciones que deben en caso de materialización.

Tabla 18. Acciones en caso de materialización.

TIPO DE RIESGO	ACCIONES
Riesgos Fiscales	Cualquier línea de defensa puede realizar el reporte de la materialización del riesgo identificado o no identificado.
	La línea de defensa que detecte la materialización debe informar a la segunda y tercera línea de defensa de la materialización del riesgo y generar alerta de las posibles consecuencias.
	El proceso responsable de la ejecución de la actividad debe hacer una descripción detallada de lo ocurrido y del impacto generado a los objetivos del proceso y de la Entidad por la materialización del riesgo.
	El proceso responsable de la ejecución de la actividad en conjunto con la Segunda línea de defensa debe revisar la identificación y valoración del riesgo, analizando las causas que lo generaron y los controles existentes con el fin de evitar que se materialice nuevamente el riesgo.
	El proceso responsable de la ejecución de la actividad basado en el

	diagnóstico de la situación presentada, establecer un plan de acción fundamentado en la actualización del mapa de riesgos.
	La segunda línea de defensa debe realizar seguimiento mensual para medir la efectividad de las acciones establecidas en el plan de acción.

Fuente: Elaboración Profesional Oficina Asesora de Planeación - OAP.

El resultado del ejercicio debe socializarse a la Línea Estratégica mediante el Comité Institucional de Control Interno – CICCI una vez culminado el periodo de seguimiento, las acciones antes descritas deben contar con el apoyo metodológico de la Oficina Asesora de Planeación.

9.3.10 Materialización de riesgos no identificados.

En el evento en que alguna de las líneas de defensa evidencie el incumplimiento de algún objetivo establecido por un proceso o la entidad que no se encuentre registrado en el Mapa de Riesgos Institucional con la posibilidad de generar pérdidas sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, se debe proceder con mesa de trabajo entre el proceso responsable y la Oficina Asesora de Planeación para proceder con la inclusión del evento en el Mapa de Riesgos Institucional cumpliendo con lo descrito en el presente Capitulo.

9.4 Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP

Con la expedición de la Ley 2195 de 2022, que hace obligatoria para la entidad la “prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional” (artículo 31), por lo anterior la Secretaría de Transparencia de la Presidencia de la República sugiere que el Programa de Transparencia y Ética Pública – PTEP cuente con un sistema de gestión que permita prevenir, detectar y corregir los eventos que amenacen 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), para esto se ha adoptado el Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, que se desarrolla a continuación.

En todo caso, de acuerdo con el parágrafo 1 del artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, la Política para la Gestión Integral de Riesgos, se articula con el PTEP y, en consecuencia, con el SIGRIP.

Teniendo en cuenta las diferentes amenazas para la integridad pública manifestadas en el presente numeral, que pueden generar peligro o daño, es necesario que, desde un enfoque

basado en riesgos, se gestionen los eventos que pueden ocurrir en la entidad, mediante la identificación, análisis y valoración de posibles eventos de riesgo asociados.

Es importante manifestar que 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, es necesario abordar los riesgos para la integridad pública de forma integral y en estrecha articulación con las demás tipologías de riesgos.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP contempla que la entidad actúe con diligencia en el conocimiento de sus contrapartes y que integre el equipo de cumplimiento, sumado a lo establecido en la presente Política para la Gestión Integral de Riesgos.

A continuación, desarrollamos cada uno de los términos que componen el SIGRIP:

9.4.1 Integridad pública

La Superintendencia de Transporte como entidad pública se expone a que sus objetivos no se cumplan como consecuencia de diferentes intereses que pueden confluir en la toma de decisiones, en la medida que se puedan privilegiar intereses propios sobre el interés general de la organización, lo que termina afectando la capacidad de la entidad para cumplir con las funciones que se le han encomendado.

En materia de integridad para la entidad, se espera que los servidores, y en general los colaboradores, dentro de un marco ético, se comporten de forma que privilegien el interés general de la entidad en todas las decisiones que deben tomar en el ejercicio de sus funciones o de los servicios que se prestan. Si bien los servidores tienen diferentes normas que establecen ese comportamiento deseado y una máxima en materia de responsabilidad, es importante recalcar que son responsables tanto de sus acciones como de sus omisiones, tal como lo establece la Constitución Política Colombiana. Manifestado lo anterior, cualquier decisión que no privilegie la entidad es un incumplimiento de la conducta deseable que constituye una actuación que pone en riesgo a la integridad.

En suma, la entidad asegura que exista y se promulgue una cultura de cumplimiento institucional, partiendo del reconocimiento del individuo y su propia ética, para asegurar que este actúe de forma íntegra, que no es otra cosa distinta que actuar con apego a la ley. Adicional a la cultura de cumplimiento que promociona la legalidad, garantizando la integridad, se adoptan medidas para gestionar todas las posibles incertidumbres que pueden poner en riesgo la garantía del interés general.

9.4.2 Amenazas para la integridad pública.

La Organización para la Cooperación y el Desarrollo Económico - ODCE, plantea la necesidad de aplicar un enfoque basado en riesgos cuando se habla de integridad pública. Manifiesta las amenazas que pueden incidir en diferentes puntos de los procesos organizacionales que terminan afectando la capacidad de una entidad para alcanzar sus objetivos, en particular, asegurar el cumplimiento de la ley. La Superintendencia de Transporte se centra en las cinco amenazas para la integridad recomendadas por dicha organización y promovidas por Función Pública:

Soborno

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 ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]". El soborno opera en dos entornos: Entrante y Saliente. El soborno Entrante corresponde al soborno suministrado al servidor de la entidad, y Saliente el soborno por parte de servidores a otros en nombre de la entidad.

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

Fraude

Corresponde a errores, omisiones, reportes/informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. 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.

Conflicto de intereses

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

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"*[3].

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 – LA/FT/FP. A través de estas prácticas y conductas se compromete la capacidad de la entidad para cumplir con sus fines, en la medida que puede ser usada 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 la institución.

9.4.3 Operación del SIGRIP

Para que el SIGRIP pueda operar adecuadamente, la Superintendencia de Transporte dispone de lo siguiente:

- El recurso financiero, tecnológico y humano para el funcionamiento de la Presente Política, el PTEP y la función de cumplimiento que en la entidad es asumida por la Oficina Asesora de Planeación.

[3] artículo 2.1.4.3.1.3 del Decreto 1081 de 2015

- El recurso humano relacionado con el funcionamiento del SIGRIP, el equipo de cumplimiento, el PTEP y la presente Política debe corresponder a profesionales universitarios con experiencia en la Gestión de riesgos mínimo de 6 meses.

- El desarrollo de dos (2) sensibilizaciones al año que permitan asegurar la toma de conciencia del personal, los líderes, el administrador, la Alta Dirección y, en general, de toda la organización, sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP. A su vez, incluir dentro de la acción de Formación del Programa de Transparencia y Ética Pública la toma de conciencia sobre:

    - Los objetivos y alcance del Sistema
    - Cada uno se sus elementos.
    - Los beneficios que tiene el Sistema para la organización.
    - Las implicaciones del incumplimiento de los requisitos del Sistema

- Publicación en la página web de la entidad del informe del SIGRIP, los resultados de su operación, así como cualquier actualización del Sistema o de algunos de sus elementos. A su vez incluir dentro de la acción de Comunicación del Programa de Transparencia y Ética Pública: Los lineamientos sobre la forma en que se comunicará, su periodicidad, los resultados del Sistema, así como cualquier actualización que se introduzca.

- Promoción de la Gestión archivística de la entidad y del sistema de gestión con los elementos necesarios para el funcionamiento del SIGRIP, permitiendo asegurar la protección de los datos personales y la confidencialidad, en el caso de la información clasificada o reservada. En cada elemento del sistema, deberá evaluarse individualmente el tratamiento que debe darse a la información documentada.

Para gestionar completamente los riesgos asociados a soborno, fraude, inadecuada gestión del conflicto de intereses, corrupción y LA/FT/FP, se requiere de tres elementos adicionales que son fundamentales para el SIGRIP: la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las herramientas de gestión del riesgo.

La estructura del SIGRIP se detalla a continuación:

Ilustración 21, Estructura del SIGRIP

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

La gestión de las amenazas para la integridad pública (fraude interno, soborno, conflicto de intereses, corrupción, LA/FT/FP) se contemplan en la presente Política, respecto a la (i) debida diligencia en el conocimiento de las contrapartes, que es efectuada a través de lo designado por el (ii) equipo de cumplimiento (función de cumplimiento) y (iii) las herramientas fortalecen la aplicación del SIGRIP, se desarrollan en la Política SARLAFT, lineamiento que complementa el desarrollo del sistema y el presente lineamiento.

9.4.4 Identificación de riesgos.

Sumado a lo descrito en el numeral "**8.4.** Identificación de riesgos", es importante manifestar que en el marco de los eventos asociados a LA/FT/FP, los puntos de riesgo se refieren a operaciones que lleva a cabo la entidad. Es decir, actividades dentro del flujo de los procesos que implican un intercambio de recursos, bien sea porque la entidad recibe un bien o servicio por el cual paga un precio, o porque entrega un bien o servicio por el cual le pagan un precio. Estas operaciones son los puntos de riesgo, que deben tenerse en cuenta para la identificación del riesgo de lavado de activos, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.

Respecto del riesgo de Corrupción 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, lo anterior debido a que son ejecutadas por personas, siendo esta la fuente de su posible exposición.

9.4.5 Identificación de áreas de impacto

Además del impacto económico y reputacional, para los riesgos de Integridad pública 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. Por lo tanto, 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 contraparte. El contagio se expresa cuando a contrapartes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar a la entidad.

Las consecuencias legales y de contagio, para efectos de determinar el impacto del riesgo, deben analizarse en términos de afectación económica, atendiendo a lo indicado en el numeral **9.6 "**Identificación de áreas de impacto" de la presente Política.

9.4.6 Identificación de áreas de factores de riesgo.

Los siguientes son los factores que intervienen para los riesgos de integridad pública:

Tabla 19, Factores de riesgo integridad pública.

Factor	Definición	Descriptores
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 empleados que afectan la Integridad Pública.	Fraude Interno
		Soborno entrante
		Soborno saliente
		Gestión inadecuada de conflicto de Intereses
		Corrupción

Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

Como factores del riesgo LA/FT/FP se tiene a las contrapartes, los productos, los canales y las jurisdicciones, 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.

9.4.7 Estructura de la Descripción del riesgo.

La descripción de los riesgos para la integridad pública mantiene la estructura definida para las demás tipologías del riesgo descrita en la **ilustración 7**. Todos inician con la formula “Posibilidad de”, seguido del impacto, la causa inmediata y la causa raíz.

Teniendo en cuenta las amenazas descritas las causas inmediatas de los riesgos para la integridad pública son el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP.

Tabla 20, Estructura del riesgo de integridad pública.

Impacto	Causa inmediata	Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	
	Soborno Saliente	
	Gestión inadecuada de Conflicto de interés	
	Corrupción	
Económico, Reputacional, Legal, Operativo o de Contagio	LA/FT/FP	Descripción de la Operación o Transacción

Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

A continuación, algunos ejemplos de riesgos de integridad pública:

- Posibilidad de afectación económica por Corrupción en la evaluación en la evaluación de los procesos de selección para la contratación de bienes y servicios

de la entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico

- Posibilidad de afectación económica por Fraude Interno en la asignación de subsidios a causa de errores, omisiones, informes inexactos o descripciones incorrectas realizados para beneficio personal o de terceros en la asignación de subsidios.
- Posibilidad de afectación reputacional por Soborno Saliente en el seguimiento a la agenda legislativa de la Entidad, a causa del ofrecimiento indebido de incentivos o recompensas para que una persona actúe o se abstenga de actuar en favor de la entidad.
- Posibilidad de afectación reputacional por Soborno Entrante al aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero, a causa de la manipulación indebida de sistema de información de asignación de citas.
- Posibilidad de afectación económica por conflicto de interés no declarado y/o declarado, pero no gestionado y/o declarado y no aceptado, a causa de decisiones en asuntos sobre los cuales la servidora o servidor público tiene un interés particular en desarrollo del comité de contratación.
- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas en las operaciones de pago de subsidios.
- Posibilidad de contagio por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de contratación directa.
- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de recaudo.

Para esta tipología de riesgos se desarrollan los siguientes numerales sin modificación:

8.7 Estructura de la descripción del Riesgo
8.8 Diseño, Análisis y Valoración de Controles
8.9 Tratamiento del Riesgo
8.10 Consolidación en el Mapa de Riesgos

9.4.8 Monitoreo y seguimiento.

El monitoreo y seguimiento se realiza acorde con lo definido en el numeral "*7 Responsabilidades*" del presente documento (Responsabilidades), en el cual se detalla lo establecido en la dimensión 7ª (Control Interno) del Modelo Integrado de Planeación y Gestión (MIPG) y a la aplicación de las líneas de defensa para identificar la responsabilidad de la gestión del riesgo. La periodicidad para el seguimiento de los riesgos y los controles se realiza acorde con lo descrito en la siguiente tabla. Es necesario reiterar que la responsabilidad de la línea de defensa estratégica es supervisar el cumplimiento de la Política para la Gestión Integral de Riesgos y evaluar su eficacia en el marco del desarrollo del Comité Institucional de Coordinación de Control Interno - CICCI.

Tabla 21. Responsabilidades Riesgos de Integridad Pública.

Responsable	Riesgos de Integridad Pública
Primera línea de defensa (líderes de procesos, Enlaces MIPG)	• Implementar, ejecutar y monitorear los controles propendiendo por su adecuado desarrollo y cumplimiento acorde a lo establecido en la matriz de Riesgos. • Gestionar y documentar de manera directa en el día a día los riesgos de su proceso o de las actividades en las que participa. <u>Cargue de Evidencias cuatrimestral:</u> A más tardar el 5° día hábil una vez terminado el cuatrimestre el líder operativo o enlace MIPG de cada uno de los procesos debe disponer las evidencias en el repositorio institucional destinado para tal fin por parte de la oficina Asesora de Planeación - OAP. A su vez debe registrar el seguimiento del comportamiento del control(es) en la herramienta indicada por la OAP
Segunda línea de defensa	<u>Periodicidad Cuatrimestral</u> Verificar y monitorear la ejecución de los controles implementados por la primera línea de defensa para mitigar los riesgos. A más tardar el 10° día hábil una vez terminado el cuatrimestre debe elaborar un informe con el monitoreo y seguimiento a los riesgos de los procesos retroalimentando al líder de proceso e informando a la tercera línea de defensa sobre el comportamiento durante el periodo de seguimiento. Debe garantizar la custodia de las evidencias en el repositorio institucional administrado por la Oficina Asesora de Planeación. El

Responsable	Riesgos de Integridad Pública
	informe debe publicarse en la Web de la Entidad para conocimiento de las partes interesadas.
Tercera línea de defensa	De acuerdo con el plan anual de auditoría aprobado - Realiza seguimiento a través de la auditoría interna (auditoría, evaluación o seguimiento), mecanismo utilizado para evaluar integralmente con independencia y objetividad la efectividad del sistema de control interno y la gestión de los riesgos llevada a cabo por la primera y segunda línea de defensa. - Las evidencias de los controles deben consultarse en el repositorio establecido por la Oficina Asesora de Planeación.

Fuente: Elaboración propia. Basado en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6, 2022

El resultado del ejercicio debe socializarse por la segunda línea de defensa (OAP) a la Línea de defensa Estratégica mediante el Comité Institucional de Control Interno – CICCI una vez culminadas las actividades mencionadas para la tercera línea de defensa.

9.4.9 Materialización de riesgos.

Dado que en cualquier momento un riesgo puede materializarse, es fundamental contar con una orientación clara sobre cómo actuar cuando esto suceda. A continuación, se describen las acciones que deben seguir en caso de materialización

Tabla 22. Acciones en caso de materialización.

TIPO DE RIESGO	ACCIONES
Riesgos de Corrupción	Cualquier línea de defensa puede realizar el reporte de la materialización del riesgo identificado o no identificado.
	La línea de defensa que detecte la materialización debe informar a la segunda y tercera línea de defensa de la materialización del riesgo y generar alerta de las posibles consecuencias.
	El proceso responsable de la ejecución de la actividad Identificar y ejecutar las acciones correctivas documentándolo en el plan de acción por procesos.
	La primera línea de defensa deber revisar y mejorar el diseño y efectividad de los controles para prevenir o mitigar una nueva

	materialización del riesgo de corrupción.
	La segunda línea de defensa (OAP) debe llevar a cabo un monitoreo mensual de las actividades propuestas.
	Tanto la segunda como la tercera línea de defensa debe verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
	La segunda línea de defensa (OAP), como la Tercer línea de defensa (OCI) debe informar a las autoridades internas y externas de la ocurrencia del hecho de corrupción.
	La segunda línea de defensa (OAP), como la Tercer línea de defensa (OCI) debe asegurar que los controles sean efectivos y oportunos, y atiendan el riesgo formulado.

Fuente: Elaboración Profesional Oficina Asesora de Planeación.

El resultado del ejercicio debe socializarse por la segunda línea de defensa (OAP) a la Línea de defensa Estratégica mediante el Comité Institucional de Control Interno - CICCI, las acciones antes descritas deben contar con el apoyo metodológico de la Oficina Asesora de Planeación.

9.4.10 Materialización de riesgos no identificados.

En el evento en que alguna de las líneas de defensa evidencie el incumplimiento de algún objetivo establecido por un proceso o la entidad que no se encuentre registrado en el Mapa de Riesgos Institucional con la posibilidad de generar pérdidas por acción u omisión generando beneficio a un tercero o particular, se debe proceder con mesa de trabajo entre el proceso responsable y la Oficina Asesora de Planeación para proceder con la inclusión del evento en el Mapa de Riesgos Institucional cumpliendo con lo descrito en el presente Capitulo

10. INDICADORES (KRI)

Los Indicadores Clave de Riesgos (KRI), hacen referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos asociada al cumplimiento de los objetivos de los procesos y por ende de los objetivos estratégicos. Un resultado desfavorable no necesariamente indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe analizar con el fin de identificar, estimar y monitorear la ocurrencia y severidad de eventos, así como posibles amenazas, por lo que se constituyen en una herramienta de apoyo para el seguimiento y monitoreo de los riesgos, ya que pueden entregar señales de alerta temprana, así como detectar tendencias o cambios en los niveles de riesgo, lo que facilita que se incorporen acciones correctivas y preventivas para minimizar sus impactos frente a posibles materializaciones.

Los indicadores clave de riesgo para la Superintendencia de Transporte corresponden a los indicadores de Gestión, los cuales cuentan con su metodología de aplicación y permiten dar cumplimiento de las actividades críticas y por ende de los objetivos de los procesos.

11. CONTROL Y SEGUIMIENTO

En el desarrollo de cada uno de los numerales de acuerdo con cada una de las tipologías de riesgos se determinan los responsables de efectuar monitoreo, seguimiento y control en los subtítulos "*Monitoreo y seguimiento*".

12. CONTROL DE CAMBIOS DEL DOCUMENTO

Versión	Fecha de publicación	Descripción
001	04-may-2026	Se asigna el documento al presente proceso, posterior a la aprobación del nuevo mapa de procesos de la entidad, en cumplimiento de la actualización de la estructura institucional.

AUTORIZACIONES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre: María Natalia Norato Mora Cargo: Contratista Oficina Asesora de Planeación	Nombre: Martha Patricia Aguilar Copete Cargo: Jefe Oficina Asesora de Planeación Nombre: Marlys Uribe Martes Cargo: Profesional Especializado Oficina Asesora de Planeación	Nombre: Martha Patricia Aguilar Copete Cargo: Jefe Oficina Asesora de Planeación

ANEXO 1

CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS

Introducción

Como resultado de la metodología de investigación que ha venido implementando el *Semillero de Investigación de la Academia de la Gestión Pública* desde el año 2018, fue posible identificar los principales *puntos de riesgo fiscal* y *circunstancias inmediatas* de dichos riesgos, mediante el estudio de: i) los avances que los diferentes órganos de control tienen frente a la definición de riesgo fiscal y la identificación de los principales riesgos fiscales en sus sujetos vigilados, ii) el estudio de fallos con responsabilidad fiscal en firme, emitidos tanto por contralorías territoriales como por la Contraloría General de la República.

Así las cosas, los *puntos de riesgo fiscal* que se enuncian en este catálogo indicativo y enunciativo corresponden a actividades que representan 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 y que potencialmente pueden generar un efecto dañoso al patrimonio público.

Este listado enunciativo y no restrictivo, también posibilita identificar y conocer las *Circunstancias Inmediatas* más comunes en la gestión pública, que se derivan de los *Puntos de Riesgo Fiscal.*

Así las cosas, como resultado del análisis de más de 130 fallos con responsabilidad fiscal tanto de contralorías territoriales como de la Contraloría General de la República, fue posible identificar 50 *puntos de riesgo fiscal* e igual número de *circunstancias inmediatas,* así*:*

Tabla 23. Puntos de riesgo fiscal.

Id Referencia	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Circunstancia Inmediata** *Situación **por la que** se presenta el riesgo*
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios

Id Referencia	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Circunstancia Inmediata** *Situación **por la que** se presenta el riesgo*
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron
19	Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad

Id Referencia	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Circunstancia Inmediata** *Situación **por la que** se presenta el riesgo*
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo

Id Referencia	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Circunstancia Inmediata** *Situación **por la que** se presenta el riesgo*
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas alcontratistas
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2022[4]

[4] Este catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias Inmediatas, es el resultado del análisis de investigaciones previas y del estudio detallado de información sobre:

(i) Fallos con responsabilidad fiscal, en firme, emitidos en los últimos 3 años, por una muestra de 10 de las contralorías territoriales mejor calificadas en 2020, según el criterio de desempeño integral, el cual corresponde a evaluación realizada por la Auditoría General de la República. *(ii)* Muestra aleatoria de fallos con responsabilidad fiscal, en firme, emitidos por la Contraloría General de la República en los últimos 3 años.*(iii)* Listado de hallazgos fiscales por temáticas, consolidado por la Auditoría General de la República, 2021.