POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

DE-PO-001

VERSIÓN 5

2023

TABLA DE CONTENIDO

1 INTRODUCCIÓN
2 Objetivo general
3 Objetivos específicos
4 Alcance
5 Definiciones
6 Marco normativo
7 Responsabilidades
8 Principios de la política
9 Declaración de la Política de Administración del Riesgo
10 Desarrollo de la Política Administración del Riesgo
10.1 Riesgos de gestión
10.2 Etapa 1. Definición de niveles de aceptación del riesgo
10.3 Estrategias para combatir el riesgo
10.4 Etapa 2. Identificación y análisis del riesgo
10.4.1 Identificación
10.4.2 Etapa 3. Valoración del Riesgo
10.4.3 Tratamiento del riesgo Inherente
10.4.4 Ubicación en Mapa de Calor
10.4.5 Valoración de Controles
10.4.6 Análisis y evaluación del control
10.4.7 Nivel de riesgo residual
10.4.8 Estrategias para combatir el riesgo residual
10.4.9 Monitoreo y seguimiento
10.4.10 Materialización de riesgos
10.5 Riesgos de Corrupción
10.5.1 Generalidades
10.5.2 Definición del Riesgo de corrupción
10.5.3 Valoración de riesgos
10.5.3.1 Análisis de la probabilidad en riesgos de corrupción
10.5.3.2 Análisis del impacto en riesgos de corrupción
10.5.4 Mapa de Calor para Riesgos de Corrupción
10.5.5 Diseño de controles
10.5.6 Nivel de riesgo (riesgo residual)
10.5.7 Tratamiento del riesgo
10.5.8 Monitoreo y seguimiento
10.5.9 Materialización de riesgos
10.5.10 SARLAFT
10.6 Riesgos Fiscales
10.6.1 Etapa 1: Definición de niveles de aceptación del riesgo
10.6.2 Etapa 2: Identificación del Riesgo
10.6.2.1 Identificación de Puntos de Riesgo Fiscales y Causa Inmediata
10.6.2.2 Identificación de la causa raíz o potencial hecho generador
10.6.3 Etapa 3: Estructuración del riesgo Fiscal
10.6.4 Etapa 4. Valoración del Riesgo
10.6.5 Tratamiento del riesgo Inherente
10.6.6 Ubicación en Mapa de Calor
10.6.7 Valoración de Controles
10.6.8 Análisis y evaluación del control
10.6.9 Nivel de riesgo residual

10.6.10 Estrategias para combatir el riesgo residual
10.6.11 Monitoreo y seguimiento
10.6.12 Materialización de riesgos
10.7 Riesgos de Seguridad de la Información
10.7.11 Monitoreo y seguimiento
10.7.12 Materialización de riesgos
10.8 Vigencia

1. INTRODUCCIÓN

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. Para el 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 presente política teniendo en cuenta que la gestión del riesgo es un factor determinante para que la Entidad 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 adecuada gestión de los riesgos, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad de la Entidad y el logro efectivo de objetivos institucionales, disminuyendo así las potenciales consecuencias negativas, y reduciendo las vulnerabilidades ante las amenazas internas y externas; adicionalmente 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 de la Entidad, lo cual se representa en la presente Política de Administración del Riesgo, 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 6 de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

Se establecen los lineamientos para la administración de los riesgos de Gestión, Corrupción, Seguridad de la Información y Fiscales. Para los riesgos de corrupción 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 de Administración del Riesgo 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 recursos públicos, el cumplimiento de los objetivos de la Entidad y mejoramiento de la prestación de los servicios a la ciudadanía.

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

2. Objetivo general

Establecer los lineamientos para la gestión del riesgo en la Superintendencia de Transporte, mediante la aplicación de las etapas de la gestión del riesgo establecidas por el Departamento Administrativo de la Función Pública permitiendo el desarrollo de la identificación, análisis, valoración, reducción y tratamiento, con el fin de proteger a la Entidad frente a posibles afectaciones y promover el cumplimiento de los objetivos establecidos por los procesos y por la Entidad.

3. Objetivos específicos

- Establecer los lineamientos para la gestión 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, corrupción, fiscales y de seguridad de la información.
- 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.
- Mejorar el direccionamiento estratégico de la Entidad
- Apoyar la toma de decisiones y la planificación en función de la gestión basada en riesgos.
- 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.

4. Alcance

El ámbito de aplicación de la Política de Administración del Riesgo contempla todos los procesos, planes, proyectos, actividades, trámites y otros procedimientos administrativos de la Superintendencia de Transporte, así como a los servidores públicos y contratistas en ejercicio de sus funciones u obligaciones; asimismo, se encuentra alineada con el objetivo y funciones de la Entidad.

5. Definiciones

Las siguientes definiciones fueron tomadas de Guía para la administración del riesgo y el diseño de controles en Entidades públicas (versión 6, 2022) emitida por el Departamento Administrativo para la Función Pública DAFP.

- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenaza:** causa potencial de un incidente no deseado, el cual puede ocasionar daño a un activo de información o proceso institucional
- **Análisis de riesgo:** proceso para comprender la naturaleza del riesgo y determinar su nivel.
- **Apetito de riesgo:** es el nivel de riesgo que la Entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección y del órgano de gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la Entidad debe o desea gestionar.
- **Bien Público:** son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así: 1) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc. 2) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.
- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la alta dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata:** circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata, pero se asocia a la misma causa inmediata.
- **Causa Raíz:** causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.
- **Confidencialidad:** propiedad de la información que la hace no disponible para que sea divulgada a individuos, Entidades o procesos no autorizados.
- **Consecuencia:** efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la Entidad, sus grupos de valor y demás partes interesadas. Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.
- **Control:** medida que permite reducir o mitigar un riesgo.
- **Desdoble:** articulación entre los objetivos estratégicos y los objetivos de los procesos en la que la agrupación de objetivos y metas de los procesos se alinea con los objetivos estratégicos y permite su monitoreo.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una Entidad.
- **Factores de Riesgo:** son las fuentes generadoras de riesgos.
- **Financiación del Terrorismo (FT):** corresponde al conjunto de acciones que permiten la circulación de recursos que tienen como finalidad la realización de actividades terroristas o que pretenden el ocultamiento de activos provenientes de dichas actividades.

- **Gestión del riesgo:** proceso efectuado por la alta dirección de la Entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la Entidad son los siguientes:
  - Apoyo a la toma de decisiones
  - Garantizar la operación normal de la organización
  - Minimizar la probabilidad e impacto de los riesgos
  - Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
  - Fortalecimiento de la cultura de control de la organización
  - Incrementa la capacidad de la Entidad para alcanzar sus objetivos
  - Dota a la Entidad de herramientas y controles para hacer una administración más eficaz y eficiente Por su parte, la norma ISO 31000 define la Gestión de Riesgos como todas aquellas acciones coordinadas para dirigir y controlar los riesgos a los que puedan estar abocadas las organizaciones, cuyo objetivo es trazar marco acción para saber qué aspecto gestionar y cómo hacerlo.
  - Gestión del riesgo fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
  - Gestor Público: es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales"[1]. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada Entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.
- **Identificación del Riesgo:** proceso para encontrar, reconocer y describir el riesgo
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** propiedad de exactitud y completitud.
- **Intereses Patrimoniales de naturaleza pública:** son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptibles de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.
- **Lavado de Activos (LA):** es el proceso mediante el cual organizaciones criminales buscan dar apariencia de legalidad a los recursos generados de sus actividades ilícitas. En términos prácticos, es el proceso de hacer que dinero sucio parezca limpio, haciendo que las organizaciones criminales o delincuentes puedan hacer uso de dichos recursos y en algunos casos obtener ganancias sobre los mismos.

- **Nivel de riesgo:** valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **Patrimonio Público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07).
- **Plan Anticorrupción y de Atención al Ciudadano:** plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las Entidades del orden nacional, departamental y municipal.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un (1) año.
- **Punto de Riesgo:** actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la Entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.
- **Recurso Público:** para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada Entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de Entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.
- **Riesgo:** efecto que se causa sobre los objetivos de las Entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Efecto que se causa sobre los objetivos de las Entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de Corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de Lavado de Activos y Financiación del Terrorismo – LA/FT:** se define como la posibilidad de pérdida o daño que puede sufrir una Entidad por su propensión a ser utilizada directamente o a través de sus operaciones, como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

- **Riesgo de Seguridad de la Información:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo Fiscal:** es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial[2]. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).
- **Riesgo Inherente:** nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **SARLAFT:** Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo.
- **Tolerancia del riesgo:** valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la Entidad.
- **Valoración del Riesgo:** proceso que comprende una serie de actividades: identificación, análisis, evaluación, administración y revisión de los riesgos.
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

---

[1] Esta definición de gestor público es armónica con la evolución que ha tenido el alcance de quien puede ser potencial responsable fiscal (art. 4 Decreto 403 de 2020 y art. 37 Ley 2195 de 2022). Adicionalmente, para mayor claridad, dentro del glosario se incluirá el concepto de gestor público, el cual se encuentra en armonía con la normativa actual sobre la materia.

[2] Concepto propuesto por Función Pública, a partir del análisis de fallos de responsabilidad fiscal y literatura investigada sobre el tema

6. Marco normativo

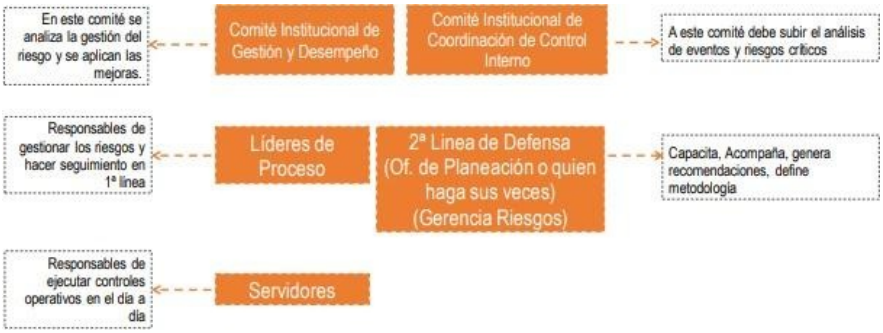
La Superintendencia de Transporte por ser una Entidad pública del orden nacional de la rama ejecutiva, debe cumplir con la regulación y la normativa que establece el Estado Colombiano en materia de administración del riesgo.

- **Ley 87 de 1993:**Por la cual se establecen normas para el ejercicio del control interno en las Entidades y organismos del Estado y se dictan otras disposiciones, artículo 2º literal a) Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. literal f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
- **Ley 489 de 1998:** Por el cual se establece el Estatuto Básico de Organización y Funcionamiento de la Administración Pública.
- **Directiva Presidencial 09 de 1999:** Se adoptan lineamientos para la implementación de la Política de Lucha contra la Corrupción.
- **Ley 1474 de 2011:** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Artículo 73. “Plan anticorrupción y de atención al ciudadano”.
- **Ley 1712 de 2014:** Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- **Decreto 1083 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Art. 2.2.21.5.4 Que establece que la Administración de riesgos es parte integral del fortalecimiento de los sistemas de control interno en las Entidades públicas.
- **Decreto 124 de 2016:** por el cual se sustituye el Titulo 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".
- **Decreto 648 de 2017:** Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, Art. 2.2.21.1.6 establece dentro de las funciones del Comité Institucional de Coordinación de Control Interno, someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.
- **Decreto 1499 de 2017:** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Adopta el Nuevo Modelo Integrado de Planeación y Gestión.
- **Decreto 1299 de 2018:** Por medio del cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector Función Pública, en lo relacionado con la integración del Consejo para la Gestión y Desempeño.
- **Decreto 454 de 2020:** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, con la incorporación de la política de gestión de la información estadística a las políticas de gestión y desempeño institucional.
- **Decreto 742 de 2021:** Por medio del cual se modifica el artículo 2.2.22.2.1. del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, con el fin de incorporar la política de Compras y Contratación Pública a las políticas de gestión y desempeño institucional.
- **Resolución 500 de 2021:** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”

- **Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas Versión 6, 2022.**

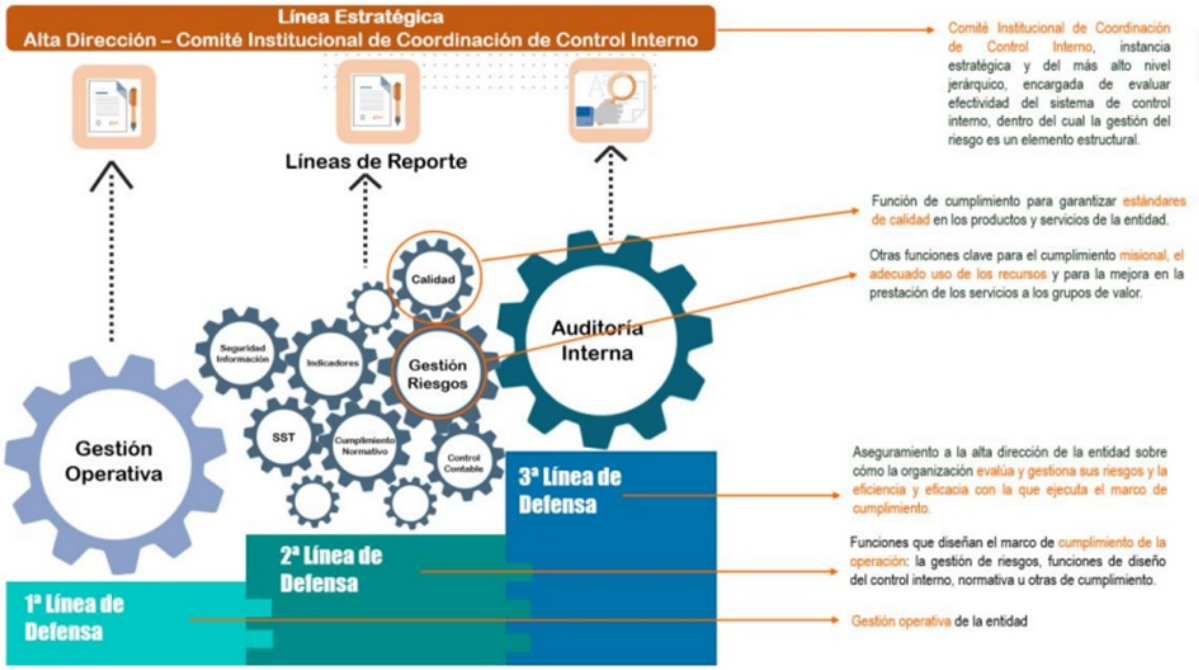
7. Responsabilidades

El Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno – CICCI establece el marco general para la adecuada gestión del riesgo en la Entidad. La operatividad de la institucionalidad para la administración del riesgo:



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

El Modelo Integrado de Planeación y Gestión – MIPG desarrolla a través de la dimensión de “Control interno” un esquema de líneas de defensa para la identificación y asignación de roles y responsabilidades frente a la gestión del riesgo. A continuación, se describe como desde la línea estratégica compuesta por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno – CICCI definen el marco general y las líneas de defensa (primera, segunda y tercera) asumiendo roles y responsabilidades con un propósito específico frente a la gestión del riesgo.



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:

Desde la Línea Estratégica (Ata Dirección) se debe definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno - CICCI. Debe aplicar el monitoreo a la Gestión del Riesgo 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.
Desde la 1ª línea de defensa todos los servidores públicos tienen la responsabilidad frente a 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 Líderes Operativos asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades. 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. Para efectos de la "*Guía para la administración del riesgo y el diseño de controles en Entidades públicas*" el Rol de Gestor de Riesgos será desempeñado por el responsable de MIPG de cada proceso.
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. 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 este encargado debe periódicamente hacer un seguimiento a todos los riesgos (de gestión, corrupción, seguridad de la información, de la Entidad, fiscales), 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 o quien hace sus veces, 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. Dando 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. A su vez 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. Verifica la publicación del mapa de riesgos en el portal web institucional. Realiza seguimiento a la gestión de riesgos (analizar causas, riesgos, eficacia y efectividad de los controles). Recomienda mejoras a la Política de Administración del Riesgo.

Fuente: Elaboración propia

8. Principios de la política

La política de administración del riesgo de la Superintendencia de Transporte, con base en lo definido por el Departamento Administrativo de la Función Pública en la versión 6 de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas y apoyándose en la Norma Técnica Colombiana NTC-ISO 31000, adopta los siguientes principios [1]:

- **Integrada:** la administración/gestión de riesgos es parte integral de todas las actividades de la organización.
- **Estructurada y exhaustiva:** posee un enfoque estructurado y exhaustivo hacia la administración/gestión de riesgos contribuye a resultados coherentes y comparables.
- **Adaptada/Ajustada:** el marco de referencia y el proceso de la administración/gestión de riesgos se adaptan y son proporcionales al contexto interno y externo de la organización relacionados con sus objetivos.
- **Inclusiva:** la participación apropiada y oportuna de las partes interesadas permite que se considere su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una administración/gestión de riesgos informada.
- **Dinámica:** los riesgos pueden aparecer, cambiar o desaparecer con los cambios del contexto interno y/o externo de la organización. La administración/gestión de riesgos anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
- **Mejor información disponible:** las entradas a la administración/gestión de riesgos se basan en información histórica y actualizada, así como en expectativas. La administración/gestión de riesgos tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información es oportuna, clara y disponible para las partes interesadas pertinentes.
- **Factores humanos y culturales:** el comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la administración/gestión de riesgos en todos los niveles y etapas.
- **Mejora continua:** la administración/gestión de riesgos mejora continuamente mediante aprendizaje y experiencia.

---

[1] Norma Técnica Colombiana NTC ISO 31000. Gestión del Riesgo: Principios y Directrices. 2018

9. Declaración de la Política de Administración del Riesgo

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, instituye en su Política de Administración del Riesgo y se compromete a:

- Establecer y apropiar la responsabilidad al interior de la Superintendencia de Transporte con el propósito de identificar, valorar, controlar, prevenir y monitorear los riesgos.
- Administrar adecuadamente los riesgos asociados a los procesos institucionales, adoptando la metodología impartida por el Departamento Administrativo de la Función Pública en la versión 6 de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.
- Identificar y tratar los riesgos de seguridad de la información tomando como insumo los activos de información de cada proceso y su clasificación a nivel de criticidad.
- Diseñar y ejecutar controles alineados para evitar la materialización de riesgos y si esto ocurre, asegurar la actuación correctiva inmediata para mitigar las posibles consecuencias a fin de mantener niveles de riesgo aceptables.
- Establecer y disponer las herramientas necesarias, con la participación de los servidores públicos y contratistas, para controlar y responder a los acontecimientos potenciales o aquellos en los que puedan desencadenar la materialización de los riesgos.
- Realizar monitoreo de los riesgos de manera periódica (periodos cortos), así como establecer seguimiento sistemático para asegurar que la gestión del riesgo sea efectiva.

A través de esta política la Superintendencia de Transporte busca promover la integridad en el ejercicio de sus funciones, 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.

10. Desarrollo de la Política Administración del Riesgo

La Política de Administración del Riesgo contempla la gestión de cuatro tipos de Riesgos:

1. Riesgos de Gestión.
2. Riesgos de Corrupción.
3. Riesgos Fiscales.
4. Riesgos de Seguridad de la Información

La matriz general de Riesgos que contempla los cuatro tipos de Riesgos debe publicarse en la página web de la Entidad.

A continuación, se explican cada uno de ellos.

10.1 Riesgos de gestión

La Superintendencia de Transporte ha definido que la metodología para la administración de riesgos de gestión se adaptará a la versión vigente de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades públicas, para este caso la versión 6 del 2022.

La administración de los riesgos de gestión se realiza en tres etapas, la primera consiste en la definición de niveles de aceptación del riesgo, etapa en la cual, la línea estratégica, define los límites del riesgo y hasta qué punto la Superintendencia de Transporte aceptará el riesgo.

En la segunda etapa, la primera línea de defensa con el acompañamiento de la segunda línea de defensa del responsable del proceso, lleva a cabo la identificación y análisis del riesgo basados en el análisis del contexto estratégico de los procesos, la identificación de los puntos del riesgo, áreas de impacto, factores, descripción y la clasificación del riesgo, lo cual permite que, a través del conocimiento de la Entidad, sus objetivos estratégicos y de proceso, determinen el impacto, las causas inmediatas y la causa raíz, para que se formulen los riesgos y así continuar con el tercer y último paso. Esta Etapa se debe efectuar como mínimo una vez al año.

En la tercera etapa, se efectúa la valoración del riesgo, donde la primera línea de defensa con el acompañamiento y asesoría de la segunda línea de defensa responsables del proceso, identifica la ubicación del riesgo inherente dentro del mapa de calor respecto a la Probabilidad e impacto, luego se construye la descripción de los controles que a su vez son calificados, con ello, después de aplicados los controles, permite fijar el riesgo residual, para determinar el desplazamiento en el mapa de calor, identificando su ubicación en riesgos bajo, moderado, alto o extremo, con lo cual se establece su manejo acorde con el nivel de aceptación definido en el primer paso, para que se implementen medidas de reducir, evitar o aceptar el riesgo.

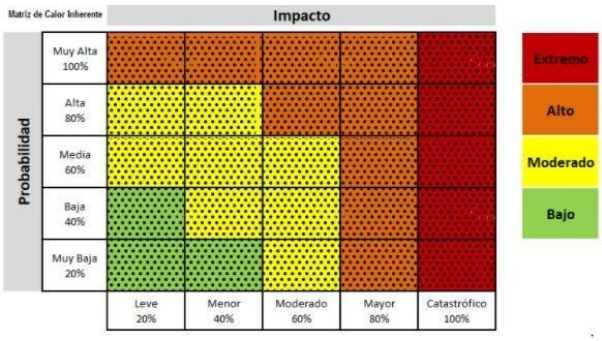
En caso de encontrarse por fuera del nivel de aceptación conduce a la Entidad a formular un plan de acción para el tratamiento del riesgo residual, así como su monitoreo y seguimiento, las etapas son:

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

10.2 Etapa 1. Definición de niveles de aceptación del riesgo

Para determinar los niveles de aceptación del Riesgo es importante conocer el mapa de calor con el cual se regirá la Gestión del Riesgo en la Entidad.

Se puede observar el mapa de calor, en la cual se obtendrá el riesgo inherente y residual de acuerdo con la probabilidad de ocurrencia (eje Y), así como su impacto (eje X) (A mayor nivel de probabilidad e impacto, mayor será la zona de Riesgo).



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

Con la aplicación de los controles se propende un desplazamiento de los niveles de probabilidad e impacto con lo cual se obtienen el nivel de riesgo residual.
Dado lo anterior y con base a lo determinado en el numeral “5. Definiciones” respecto a “Capacidad de riesgo”, se establece que el máximo valor del nivel de riesgo que la Entidad puede soportar es la Zona de Riesgo Extrema, siempre y cuando se apliquen controles sin excepción. Caso contrario el evento de Riesgo debe evitarse.

Con relación al nivel de aceptación de Riesgo se estipula que la Zona Baja corresponderá a la ubicación en la que los Riesgos Inherentes o Residuales serán aceptados y no requerirán tratamiento adicional.

10.3 Estrategias para combatir el riesgo

Como complemento a lo anterior se determinan las decisiones que se toman frente a un determinado nivel de riesgo, pueden ser: aceptar, reducir o evitar. De acuerdo con lo anterior, la Superintendencia de Transporte ha definido los niveles de aceptación de riesgos y las decisiones para combatirlos. Dependiendo de la zona de riesgo residual donde se ubique se da tramite

Zona de Riesgo Residual	Riesgos de Gestión
Bajo	Aceptar el riesgo se administra con las actividades propias de cada proceso.
Moderado	Se debe incluir en el mapa de riesgo institucional estableciendo acciones de control preventivas, detectivas y/o correctivas que permitan Reducir la probabilidad e impacto del riesgo.
Alto	Se debe incluir en el mapa de riesgo institucional definiendo acciones de control preventivas, detectivas y/o correctivas que permitan Reducir la probabilidad e impacto de ocurrencia del riesgo.
Extremo	Se incluye el riesgo en el Mapa de Riesgos Institucional, implantando acciones de control preventivas, detectivas y/o correctivas que permitan Reducir la probabilidad e impacto de ocurrencia del riesgo. ó No fijar acciones y Evitar la actividad que da lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.

Fuente: Elaboración propia de la Oficina Asesora de Planeación.

10.4 Etapa 2. Identificación y análisis del riesgo

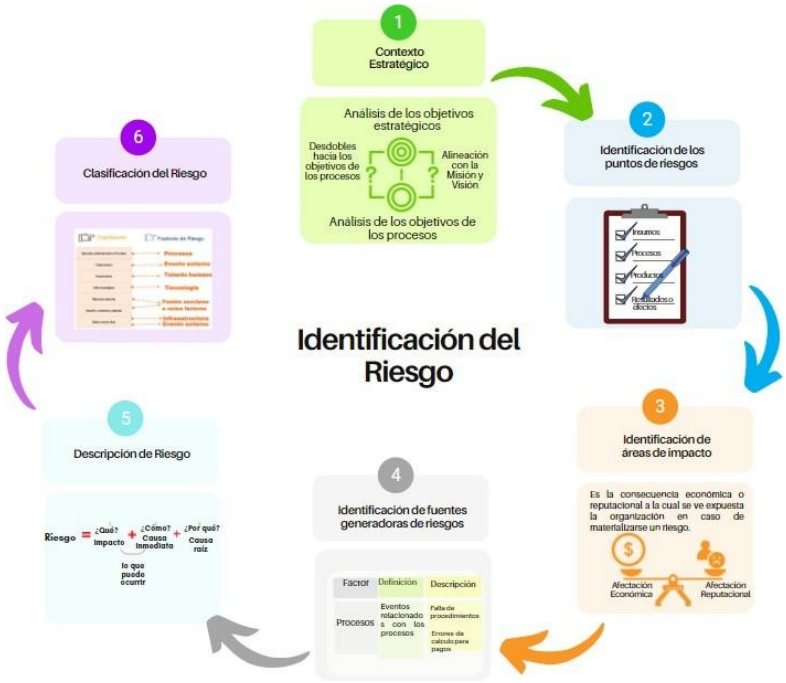
En esta etapa, los líderes de proceso o de enlace con MIPG en compañía de la Oficina Asesora de Planeación toman como referencia los riesgos que se encuentran vigentes en el mapa de riesgos, confirmando su continuidad o no dentro de la matriz. Posteriormente, con apoyo del contexto estratégico del proceso que debe actualizarse como mínimo una vez en la vigencia y el cual debe estar acorde con la caracterización y el objetivo definido para que en el proceso se determine la necesidad de incluir, ajustar, mantener y/o inactivar los riesgos identificados.

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 clara de la inactivación del riesgo del proceso por parte de su líder operativo, el hecho debe registrarse en el informe de seguimiento emitido por la Segunda Línea de Defensa del responsable del proceso.

10.4.1 Identificación

Para lograr identificar los riesgos que pueden afectar al proceso por situaciones internas o externas se aplicarán los pasos definidos en la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas vigente” de la Función Pública, los cuales se describen a continuación:



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

Paso 1. Contexto Estratégico

En este paso, se revisan y analizan los objetivos estratégicos, verificando su alineación con la misión y visión, su articulación y desdobles con los objetivos de los procesos.

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

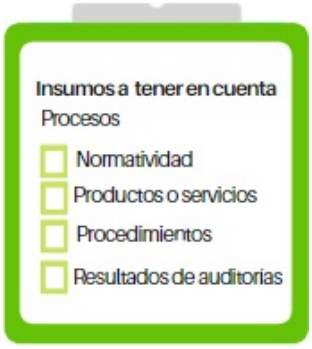
Como se observa, esta actividad, debe realizarse durante y después de la formulación de la planeación estratégica, confirmando los objetivos de los procesos formulados.

Los objetivos de los procesos se definen y redactan dando respuesta a los conceptos de calidad enfocados en resultados, recursos e impactos esperados, estableciendo claramente en su redacción el: “porque”, “mediante” y “para que” de acuerdo con las preguntas que se observan:

Objetivo del proceso			
Preguntarnos	¿ Qué hacemos ?	¿Por medio de qué lo hacemos ?	¿Para qué lo hacemos ?
Redactar	Que	Mediante	Para qué
Medir	La Eficacia (resultado)	Eficiencia (recursos)	Efectividad (impacto)

Fuente: Elaboración propia de la Oficina Asesora de Planeación

Paso 2. Identificación de los puntos de riesgo.
Son las actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo. A continuación, se observa que en la identificación de los puntos de riesgo se tendrá como insumos la normatividad, productos o servicios, procedimientos, resultados de las auditorías internas y externas, y demás documentos del proceso.



Fuente: Elaboración propia, basado en la guía para la administración del riesgo y el diseño de controles en Entidades públicas. Versión 6, 2022

Paso 3: Identificación de áreas de impacto
El área de impacto es la afectación económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Ambas repercusiones pueden afectar a la Superintendencia de Transporte, es importante tener presente que se pueden presentar en conjunto o por separado.

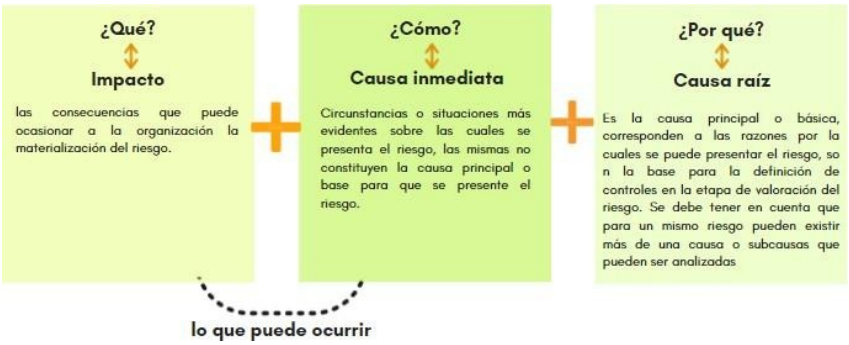
Paso 4. Identificación de áreas de factores de riesgo
Las áreas de factores de riesgos son las fuentes generadoras de estos, por lo cual la Superintendencia de Transporte revisó cada uno de los factores de riesgos propuestos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas y los adoptó en la Entidad, identificando los factores de riesgos, representados en la siguiente tabla.

Factor	Definición	Descripción
Procesos	Evento relacionado con errores en la actividad que deben realizar los servidores de la organización.	Falta de procedimientos o procedimientos desactualizados Errores de autorización Errores en cálculos para pagos interno o externo Falta de capacitación, temas relacionados con el personal
Talento Humano	Incluye seguridad y salud en el trabajo, se analiza posible dolo e intención frente a la corrupción	Hurto activos Posibles comportamientos no éticos de los empleados Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad	Daño de equipos Caida de aplicaciones Caida de redes Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes Incendios Inundaciones Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad Asalto a la oficina Atentados, vandalismo, orden público

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

En el caso que durante la evaluación y definición de riesgos se identifiquen nuevos factores estos se incluirán y actualizarán en la tabla de factores.

Paso 5: Descripción del Riesgo
Con el propósito que el riesgo sea claro y de fácil comprensión para las personas de la Entidad, así como para personas externas a ella, debe poseer la siguiente estructura en su redacción contemplando el impacto, causa inmediata y causa raíz, tal como se ilustra en la siguiente figura.



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

Para facilitar la descripción del riesgo, se plantean los elementos que debe poseer la redacción del riesgo y que se deben tener en cuenta para garantizar la estructura propuesta:

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

Al redactar el riesgo es importante establecer los siguientes aspectos:

- **¿Qué puede suceder?: Permite establecer en términos generales el evento o situación que puede obstaculizar el cumplimiento del objetivo del proceso o de la Superintendencia de Transporte.**

Ejemplo: Incumplir con la publicación de los planes, programas y proyectos en los tiempos establecidos.

Posteriormente, se analiza la estructura del Riesgo iniciando por el Impacto, la causa inmediata y la causa raíz, de la siguiente forma:

- **Impacto (Que): Hace referencia a las consecuencias que puede ocasionar a la organización la materialización del riesgo. En esta casilla usted deberá seleccionar si el impacto es:**

- Económico
- Reputacional
- Económico y Reputacional o Reputacional y Económico.

Ejemplo: Económico y Reputacional.

- **Causa inmediata (Cómo): Hacen referencia a las 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.**

Ejemplo: Suministrar información incompleta e inválida para la publicación.

- **Causa raíz (Por qué): Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo.**

Ejemplo: Inadecuada planeación para contar con los planes, programas y proyectos validados para publicar en los tiempos establecidos.

Finalmente, se procede con la agrupación de los anteriores campos así:

- **Descripción del riesgo: compila lo registrado en los anteriores campos teniendo en cuenta la estructura, representada de la siguiente forma:**

Posibilidad de ... ± Impacto para la Entidad (Qué) ± Causa Inmediata (Cómo) ± Causa Raíz (Por qué)

Ejemplo: Posibilidad de daño económico y reputacional por suministrar información incompleta e inválida para la publicación, debido a inadecuada planeación para contar con los planes, programas y/o proyectos validados para publicar en los tiempos establecidos.

Paso 6. Clasificación del Riesgo

Es pertinente agrupar o clasificar los Riesgos de acuerdo con el tipo de pérdida o fallo que se presente, se ha contemplado adoptar lo descrito en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas y que se detallan en la siguiente Figura.

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

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

Una vez clasificados se permite obtener y determinar con mayor claridad el Factor que incide para la generación del Riesgo, la relación entre ellos se representa en la siguiente figura:

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

Es importante contar con la clasificación del riesgo y los Factores de Riesgo tomando la agrupación de acuerdo con su naturaleza, lo cual es visible en la matriz de Riesgo y permite determinar el grado de afectación por cada uno de los factores y eventos que se pueden presentar en la Entidad.

10.4.2 Etapa 3. Valoración del Riesgo

En esta etapa se establece el nivel de probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el propósito de estimar la zona de riesgo inicial o inherente en el mapa de calor compartido en el numeral “10.2 Etapa 1. Definición de niveles de aceptación del riesgo”. Los siguientes son los niveles para valorar ambos aspectos:

- Niveles para calificar la probabilidad

Para determinar la probabilidad, la cual es entendida como la posibilidad de ocurrencia del riesgo, la cual estará asociada a la exposición del proceso o actividad que se esté analizando respecto al Riesgo. De este modo, la probabilidad corresponde al número de veces que se pasa por el punto de riesgo en el periodo de 1 año. A continuación, presenta los criterios para definir la probabilidad.

Nivel de 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 de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6, 2022.

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.

- Niveles para calificar el impacto

La calificación del impacto se debe aplicar en relación al tipo de afectación que se detectó en la descripción del Riesgo, respecto a si es económica o reputacional o ambas. Se debe efectuar la selección de acuerdo con los rangos que se detallan.

Niveles de Impacto	Afectación Económica	Afectación Reputacional	Impacto
Leve	Afectación menor a 199 SMLMV	El riesgo afecta la imagen de algún área de la Entidad.	20%
Menor	Entre 200 y 499 SMLMV	El riesgo afecta la imagen de la Entidad internamente, de conocimiento general nivel interno, de directivos y/o de proveedores.	40%
Moderado	Entre 500 y 999 SMLMV	El riesgo afecta la imagen de la Entidad con algunos usuarios de relevancia frente al logro de los objetivos.	60%
Mayor	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.	80%
Catastrófico	Mayor a 5.000 SMLMV	El riesgo afecta la imagen de la Entidad a nivel nacional, con efecto publicitario sostenido a nivel país	100%

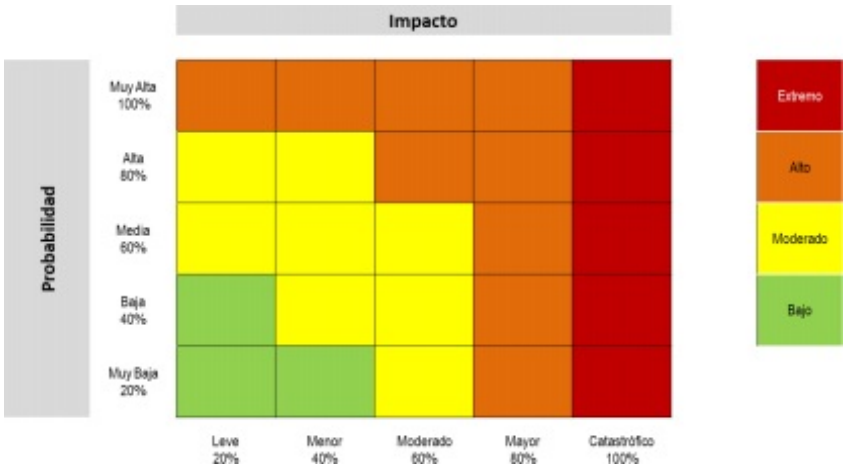
Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Versión 6, 2022.

10.4.3 Tratamiento del riesgo Inherente

Luego de la valoración de la probabilidad y el impacto de los riesgos, que busca determinar la zona de riesgo inherente, se procede con la ubicación del Riesgo en el Mapa de Calor; ejercicio que se complementa con la aplicación o no de controles, dependiendo de lo establecido en el numeral "*10.3 Estrategias para combatir el riesgo*". La aplicación y ejecución de controles determina el nivel de Riesgo residual.

10.4.4 Ubicación en Mapa de Calor

Utilizando la Matriz de Calor riesgo socializado en el numeral "*10.2 Etapa 1. Definición de niveles de aceptación del riesgo*" y tomando los resultados obtenidos en el numeral "*10.4 Etapa 3. Valoración del Riesgo*" se obtiene la zona de riesgo Inherente. El siguiente es el mapa de calor que se utiliza para los Riesgos de gestión.



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

La Oficina Asesora de Planeación recomienda la estructuración como mínimo de un control para cada riesgo.

10.4.5 Valoración de Controles

Como medida para mitigar el riesgo y lograr reducir o evitar su materialización se deben construir controles, los cuales deben cumplir con la estructura que permita determinar que es una actividad o mecanismo que cumpla como punto de verificación o validación.

Para su construcción, se debe contar el apoyo de los líderes de proceso, lideres operativos o personal experto en el que hacer, con el fin ~~de~~ que sean identificados y descritos de forma detallada. Cuando se identifique un control, se deberá redactar con la estructura que se observa a continuación:

Fuente: Elaboración propia de la Oficina Asesora de Planeación.

De igual forma, es muy importante que al describir el control se realice de forma detallada contemplando el propósito, permitiendo un claro entendimiento para cualquier persona, así mismo, deberá identificar cual es el producto que permite evidenciar la aplicación de dicho control.

Para que un control este adecuadamente diseñado y que su implementación sea efectiva a la hora de mitigar un riesgo, éste debe cumplir con los siguientes lineamientos:

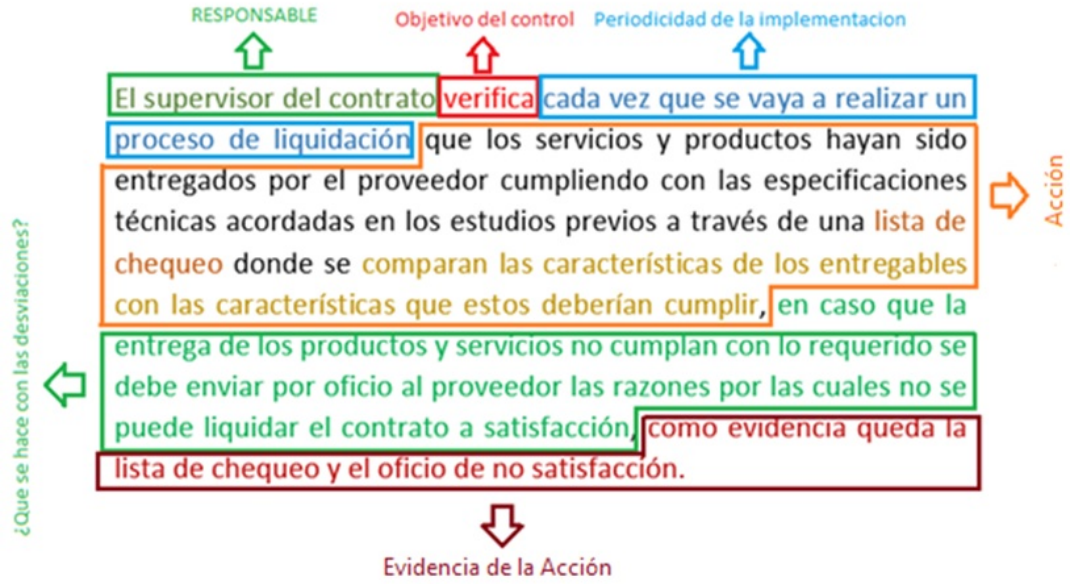
Debe tener un responsable de su ejecución, identificar el cargo del servidor que ejecuta el control, en caso que sean controles automáticos se identifica el sistema que realiza la actividad. (Evitar colocar áreas generales o nombres propios), por ejemplo: responsable de inventarios.

En la descripción del control se debe especificar como se ejecuta la Acción del control.

El complemento con detalles adicionales que permitan identificar claramente la ejecución del control:

- La ejecución del control debe tener un soporte documental, por ejemplo, una base de datos, una lista de chequeo, un acta de reunión, etc.
- En la definición del control, se debe especificar cuál es la periodicidad de la aplicación de este; por ejemplo: el coordinador debe revisar (mensualmente, trimestralmente, cada vez que se presente…).
- La definición debe incluir cuál es el Objetivo del control (valida, coteja, compara, concilia…).
- La definición del control debe incluir en que situaciones se presentan desviaciones entre el resultado esperado, el resultado obtenido y que acciones se deben tomar si se presentan dichas desviaciones.

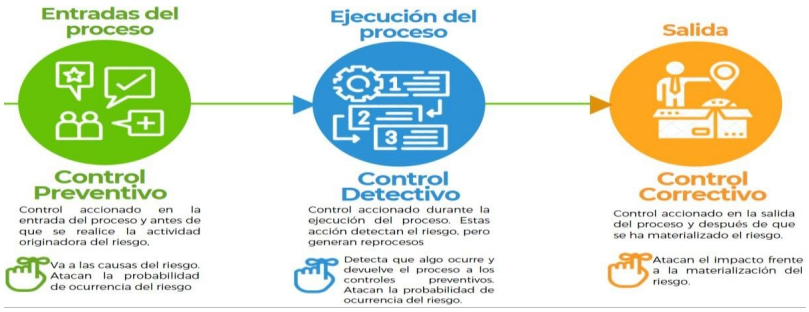
Se comparte un ejemplo de control, el cual cuenta con la estructura necesaria para poder incluirse en la matriz de Riesgos de Gestión:



Fuente: Elaboración propia de la Oficina Asesora de Planeación.

Se debe identificar el tipo de control de acuerdo con el momento en el cual se ejecuta o activa dentro del procedimiento que genera el riesgo. Son 3 momentos en los cuales se puede efectuar un control y este puede llegar a ser Preventivo, Detectivo o Correctivo.

Los dos primeros permiten desplazamiento de probabilidad en el mapa de calor y el ultimo permite movimiento para el impacto. Se detalla el funcionamiento de cada uno. Se recomienda en lo posible tener un control de cada tipo que permita la adecuada gestión del control.



Fuente: Elaboración propia de la Oficina Asesora de Planeación.

10.4.6 Análisis y evaluación del control

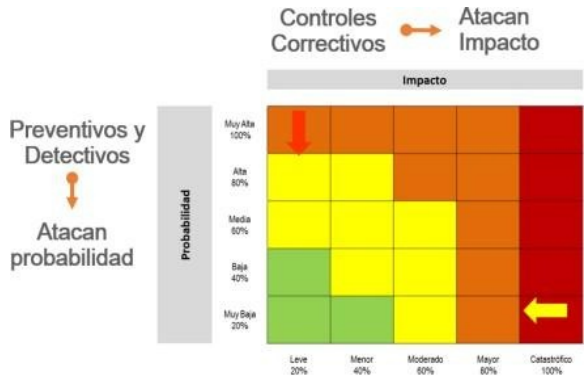
Una vez se tenga descrito el control, se realiza su valoración de acuerdo con los atributos que se describen a continuación:

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 de Formalización		Responsable	Cuenta con responsable del Control	-
		Objetivo	Cuenta con un Objetivo	-
		Evidencia	Se tiene Evidencia de la ejecución del control	-
		Desviaciones	Se tienen en cuenta las desviaciones de la ejecución del control	-
		Periodicidad de ejecución	Se ejecuta con una periodicidad adecuada	-

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

Con los controles y el tipo de control, se busca desplazar el riesgo inherente al riesgo residual dependiendo de su tipología se percibirá el movimiento. Los atributos informativos no brindan valor o peso a la ejecución del control, pero son determinantes para poder incluirlos en la matriz de Riesgos. En caso de no contar con algún atributo se debe proceder con la reformulación del control.

Una vez valorados los controles, el riesgo inherente cambiará a riesgo residual, en la medida que los controles preventivos y detectivos atacan la probabilidad de ocurrencia y los controles correctivos el impacto, como se ilustra.



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

10.4.7 Nivel de riesgo residual

El nivel del riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente. La aplicación de los controles mitiga el riesgo de forma acumulativa, esto quiere decir que, una vez se aplica el valor del primer control, el siguiente se aplicará con el valor resultante de la aplicación del primero. Las siguientes son las fórmulas aplicadas para probabilidad e impacto:

PROBABILIDAD

La formulación es la siguiente:

Probabilidad Inherente = PI
Valoración Control Preventivo = VCP
Probabilidad Residual$_1$ = PR$_1$

Para las situaciones en las cuales se cuente con controles Detectivos se procederá continuara con la aplicación de la Formula:

Probabilidad Residual$_1$ = PR$_1$
Valoración Control Detectivo = VCD
Probabilidad Residual$_n$ = PR$_n$

Para los casos en los cuales se cuente con más controles se continuará ejecutando la formula hasta agotar la cantidad de Controles estructurados siempre otorgando prioridad a las tipologías con el siguiente Orden: Preventivo-Detectivo.

IMPACTO

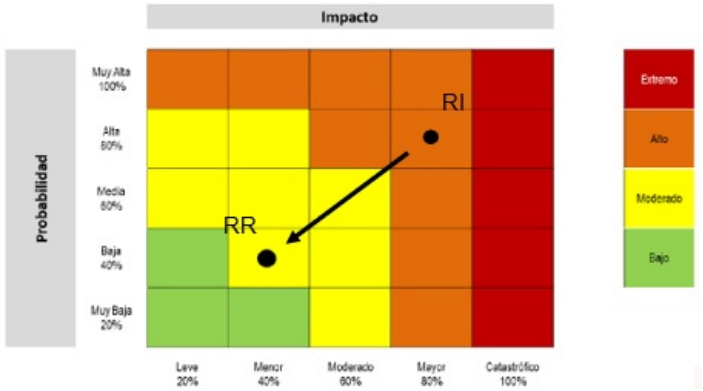
La formulación es la siguiente:

Impacto Inherente$_1$ = II$_1$
Valoración Control Correctivo = VCC
Impacto Residual$_n$ = IR$_n$

Con lo anterior, se determinará la posición del riesgo después de la ejecución del (los) control(es) considerando que están correctamente diseñados y que en efecto estos mitigan las causas, evitando que el riesgo se materialice. Se debe propender la formulación de un control por cada tipología Preventivo-Detectivo-Correctivo.

10.4.8 Estrategias para combatir el riesgo residual

Si una vez aplicados los controles al Riesgo Inherente (RI), da como resultado que el riesgo residual (RR), se ubica en el mapa de calor en una zona diferente a baja, se deben efectuar un tratamiento al riesgo residual correspondiente a la aplicación de un plan de acción. En la figura se detalla el movimiento ideal de un Riesgo Inherente a Residual.



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

Dada la Zona de Riesgo Residual luego de la ejecución de controles, el tratamiento al riesgo es el siguiente:

- Aceptar el riesgo: Valido únicamente para aquellos cuya Zona de Riesgo Residual es Baja no se aplica ninguna acción adicional a la ejecución permanente del control que se tiene estipulado asumiendo el mismo conociendo los efectos de su posible Materialización.
- Reducir el riesgo: Para aquellos cuya Zona de Riesgo Residual sea diferente a Baja, se deberán toman acciones mediante Transferencia o Mitigación previa realización de un análisis de la situación dejando evidencia en la Matriz de Riesgos:
    - Mitigar: Esto se logra por medio de acciones que aminoren el nivel de Riesgo.
    - Transferir: Estrategia de tercerización del proceso o traslado del riesgo a través de Seguros o Pólizas. La Responsabilidad económica recaerá sobre el tercero. Sin embargo, se mantiene la Responsabilidad reputacional.
- Evitar el riesgo: Se determina no asumir el riesgo por lo cual se elimina la ejecución de las actividades que faciliten la materialización.

10.4.9 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, los controles y el Plan de Acción se realiza acorde con lo descrito en la siguiente Tabla.

Responsable	Riesgos de Gestión
Primera línea de defensa (líderes de procesos, Enlaces MIPG)	• Implementar, ejecutar y monitorear los controles y el plan de acción 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 Trimestral:</u> A más tardar el 10° día hábil una vez terminado el trimestre, el líder operativo o enlace 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.
Segunda línea de defensa	<u>Periodicidad trimestral</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 trimestre 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 por el CICCI.</u> • 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. Basado en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6, 2022

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

10.4.10 Materialización de riesgos

Considerando la posibilidad materialización de un riesgo, es fundamental contar con una clara orientación sobre cómo actuar en caso de que esto ocurra. Las siguientes son las acciones que debe seguir la primera línea de defensa en caso de materialización.

TIPO DE RIESGO	ACCIONES
Riesgos de Gestión	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 mejoramiento fundamentado en el mapa de riesgos.
	Realizar seguimiento mensual para medir la efectivad 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, las acciones antes descritas deben contar con el apoyo metodológico de la Oficina Asesora de Planeación.

10.5 Riesgos de Corrupción

El riesgo de corrupción está definido como "*la posibilidad que; por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado*". Lo anterior permite detectar que estas prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos.

La Superintendencia de Transporte, determina que todos los procesos deben identificar, analizar y gestionar los riesgos de corrupción, es decir, no es posible que algún proceso no contemple o no tenga riesgos de corrupción.

10.5.1 Generalidades

Para la Gestión de los Riesgos de Corrupción se deben tener en cuenta los siguientes aspectos generales:

1. El líder de procesos y Enlace MIPG junto con su equipo de trabajo verifican anualmente los posibles eventos de Riesgos de Corrupción en compañía del apoyo metodológico de la Oficina Asesora de Planeación, con el fin de confirmar, modificar o inactivar los Riesgos de la matriz institucional, lo cual quedara registrado en acta de reunión con las decisiones tomadas. De igual forma, en el transcurso de la vigencia se podrán llevar a cabo los ajustes y modificaciones adicionales orientadas a mejorar el mapa de riesgos de corrupción, lo cual debe contar con Acta de reunión debidamente diligenciada y firmada, indicando lo correspondiente.
2. La oficina Asesora de Planeación, lidera la metodología y acompaña a los responsables de los procesos en la gestión de los riesgos de corrupción. A su vez, consolida el mapa de riesgos de corrupción realizando el seguimiento y monitoreo a los riesgos identificados.
3. El mapa de riesgos de corrupción debe estar disponible para consulta en la web de la Entidad, permitiendo que las partes interesadas lo consulten y puedan poner a consideración su formulación permitiendo su conocimiento y la construcción de apreciaciones o propuestas que permitan fortalecerlo. Se deben publicar en la página web de la Entidad, en la sección de transparencia y acceso a la información pública de acuerdo con lo establecido en el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015, a más tardar el 31 de enero de cada año.
4. En concordancia con la cultura del autocontrol al interior de la Entidad, los líderes de los procesos junto a los Enlaces MIPG y su equipo de trabajo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
5. El jefe de la Oficina de Control Interno – OCI debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna (auditoría, evaluación o seguimiento) analice las causas de los riesgos de corrupción y la efectividad de los controles incorporados.

10.5.2 Definición del Riesgo de corrupción

A continuación, se establecen los parámetros para la definición de los riesgos de corrupción:

- Los riesgos de corrupción se establecen sobre procesos.
- Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos, por lo cual debe estar descrito de manera clara y precisa.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, la redacción del Riesgo debe permitir la identificación de los componentes ilustrados.

Fuente: Adaptado de la Secretaria de Transparencia de la Presidencia de la República

En la descripción de los riesgos de corrupción deben concurrir todos los componentes:

acción u omisión + uso de poder + desviación de la gestión de lo público + el beneficio privado.

10.5.3 Valoración de riesgos

Para la valoración del riesgo de corrupción es importante el cálculo de la probabilidad e impacto, esta se realizará acorde a lo definido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - Riesgos de Gestión, Corrupción y Seguridad Digital versión 6. Como se informa a continuación:

10.5.3.1 Análisis de la probabilidad en riesgos de corrupción

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

Criterios para calificar la probabilidad

El análisis de probabilidad de los riesgos de corrupción determina qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, para ello se utilizan los siguientes criterios establecidos.

Nivel	Descriptor	Descripción	Frecuencia
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales	No se ha presentando en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
4	Probable	Es viable que el evento ocurra en la mayoría de circustancias.	Al menos 1 vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circustancias	Más de 1 vez al año.

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital versión 6

10.5.3.2 Análisis del impacto en riesgos de corrupción

El impacto se debe definir y analizar a partir de las consecuencias identificadas en la fase de descripción del riesgo, por lo cual, la Superintendencia de Transporte se acoge a lo definido en la guía de FP versión 5, y que se detalla en la siguiente tabla.

Si el riesgo de corrupción se materializa, podría...	Respuesta	
	Sí	No
1. ¿Afecta al grupo de funcionarios del proceso?	☐	☐
2. ¿Afecta el cumplimiento de metas y objetivos de la dependencia ?	☐	☐
3. ¿Afecta el cumplimiento de la misión de la entidad ?	☐	☐
4. ¿Afecta el cumplimiento de la misión del sector al que pertenece la entidad ?	☐	☐
5. ¿Genera pérdidas de confianza de la entidad, afectando su reputación?	☐	☐
6. ¿Génera pérdida de recursos económicos ?	☐	☐
7. ¿Afecta la generación de los productos o la prestación de servicios ?	☐	☐
8. ¿Da lugar al detrimento de calidad de vida de la comunidad por pérdida del bien, servicios o recursos públicos ?	☐	☐
9. ¿Genera pérdida de información de la entidad ?	☐	☐
10. ¿Genera intervención de los órganos de control, de la Fiscalia u otro ente?	☐	☐
11. ¿Da lugar a procesos sancionatorios ?	☐	☐
12. ¿Da lugar a procesos disciplinarios ?	☐	☐
13. ¿Da lugar a procesos Fiscales ?	☐	☐
14. ¿Da lugar a procesos penales ?	☐	☐
15. ¿Genera pérdida de credibilidad del sector ?	☐	☐
16. ¿Ocasiona lesiones fisicas o pérdida de vidas humanas ?	☐	☐
17. ¿Afecta la imagen regional?	☐	☐
18. ¿Afecta la imagen nacional?	☐	☐
19. ¿Genera daño ambiental?	☐	☐

Fuente: Tomado de la guía para la administración del riesgo y el diseño de controles en Entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital versión 4

Es importante tener en cuenta que, si durante el análisis y valoración de los riesgos, la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.

Estas preguntas deben resolverse para cada uno de los riesgos de corrupción identificados. Una vez se complete el cuestionario se deberán contar las respuestas positivas y valorar el impacto de acuerdo con la siguiente tabla, así:

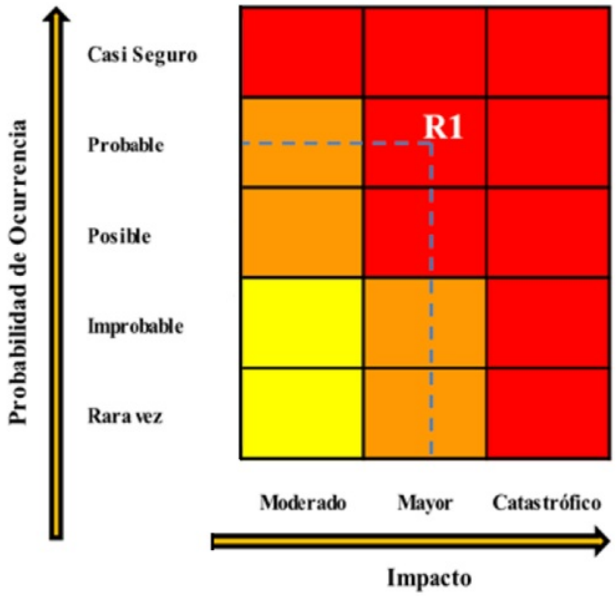
Impacto Moderado	Responder afirmativa de **1 a 5** pregunta(s) genera un impacto moderado	Medianas consecuencias sobre la entidad
Impacto Mayor	Responder afirmativa de **6 a 11** pregunta(s) genera un impacto mayor	Altas consecuencias sobre la entidad
Impacto Catastrófico	Responder afirmativa de **12 a 19** pregunta(s) genera un impacto catastrófico.	Consecuencias desastrosas para la entidad

Fuente: Adoptado de la guía para la administración del riesgo y el diseño de controles en Entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital versión 4

10.5.4 Mapa de Calor para riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos.

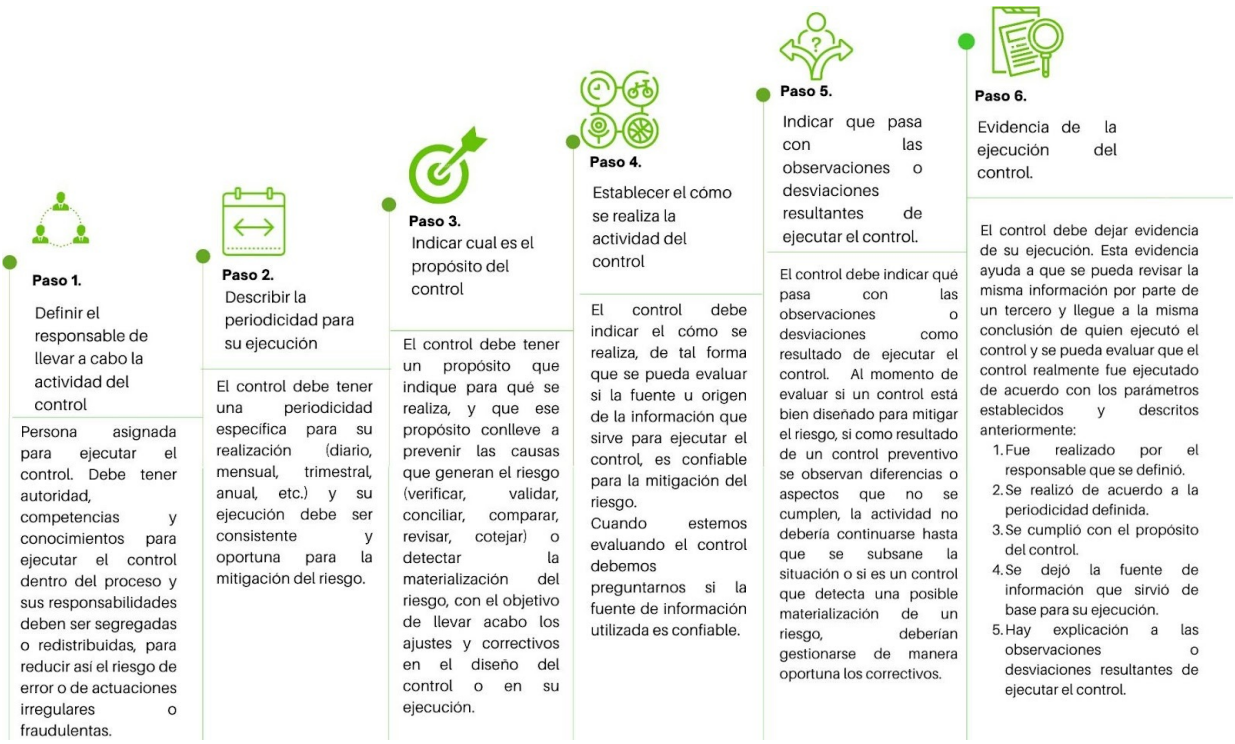
El punto de intersección resultante de la probabilidad de ocurrencia (Rara vez, Improbable, Posible, Probable, Casi seguro) y el impacto (Insignificante, Menor, Moderado, Mayor, Catastrófico) determina el nivel del riesgo inherente como se ilustra en la figura.



Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas. Versión 6

10.5.5 Diseño de controles

Los controles que se estructuren para mitigar los Riesgos de Gestión deben cumplir con una estructura que permita establecer su efectividad. Los Riesgos de Corrupción únicamente pueden ser gestionados por controles preventivos y detectivos. Las características que deben tener los controles son:



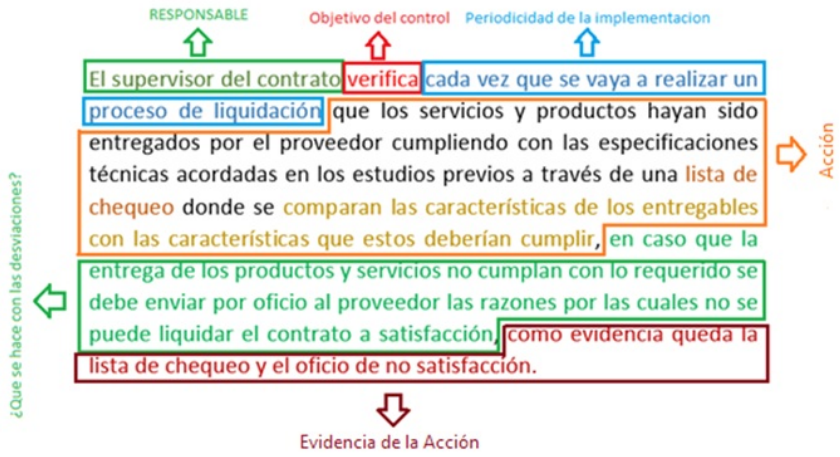
Fuente: Adoptado de la guía para la administración del riesgo y el diseño de controles en Entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital versión 6.

Notas Aclaratorias:

- Para aquellos casos en los cuales la actividad control represente el manejo de información reservada o clasificada deberá mencionarse dentro de la actividad control y se deberá aclarar dentro del mismo que tipo de evidencia se recibirá. Dicha información debe ser acorde a lo dictaminado en la Ley 1712 del 2014 y lo desarrollado en el "*Índice de Información Clasificada y Reservada*" de la Entidad.
- Se recomendará el uso de Matrices gerenciales para los casos en los cuales se presente manejo de información reservada o clasificada, con las cuales se logre evidenciar la ejecución de las actividades de control.

- La manera en la cual se lleva a cabo su implementación debe estar documentada en alguno de los documentos oficializados del proceso (por ejemplo, en un procedimiento, un manual, un instructivo, etc.), sin querer decir que la existencia de dicho documento donde esta consignada esta información sirva como el control per se (por si mismo).
- Cada causa del riesgo debe tener por lo menos un control asignado a su mitigación.

A continuación, se observa la estructura recomendada para los controles.



Fuente: Elaboración Profesional de la Oficina Asesora de Planeación - OAP

Valoración de los controles
Para valorar los controles, se tendrá en cuenta la siguiente estructura en la cual de acuerdo con la información registrada en el cuerpo del control se determinará su peso.

Criterio de evaluación.	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del Responsable.	Asignado	15
	No Asignado	0
1.2 Segregación y Autoridad del Responsable.	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un Control	0
4. Como se realiza la actividad de control.	Confiable	15
	No Confiable	0
5. Que pasa con las observaciones o desviaciones.	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente.	0
6. Evidencia de la ejecución del control.	Completa	10
	Incompleta	5
	No Existe	0

Fuente: Adoptado de la guía para la administración del riesgo y el diseño de controles en Entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital versión 6.

Esta evaluación, mide cada una de las variables de los controles, el resultado de cada variable de diseño afectará la calificación del diseño del control y asignará un puntaje según la tabla:

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO - PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Riesgos de Gestión, Corrupción y Seguridad Digital versión 6.

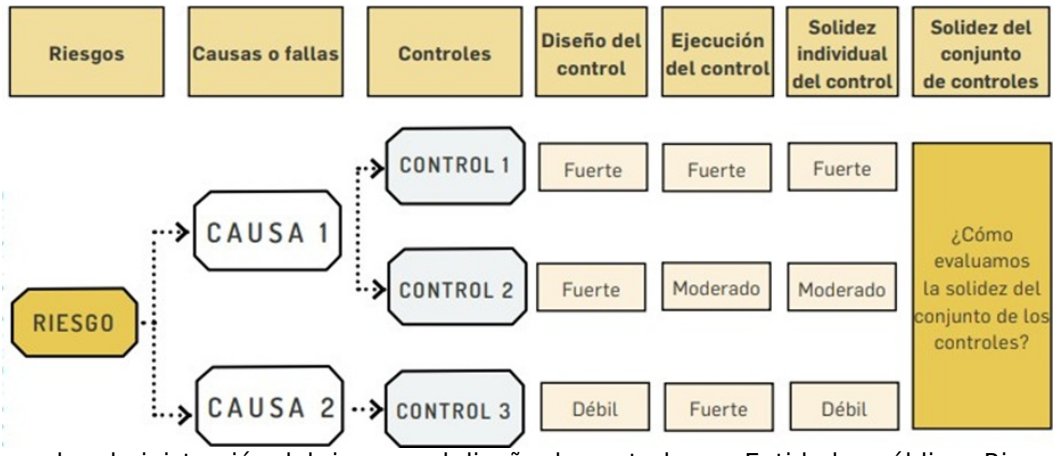
Análisis y evaluación de los controles

En esta etapa se consolida el conjunto de los controles, para evaluar si estos de manera individual y en conjunto ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles. En la evaluación del diseño y ejecución de los controles las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se referencia a continuación.

PESO DEL **DISEÑO** DE CADA CONTROL	PESO DE LA **EJECUCIÓN** DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL **FUERTE:100 MODERADO:50 DÉBIL:0**	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL **SÍ / NO**
fuerte: calificación entre 96 y 100"	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Riesgos de Gestión, Corrupción y Seguridad Digital versión 6

En este mismo sentido y teniendo en cuenta que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo, teniendo en cuenta la solidez de los controles como se detalla.



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Riesgos de Gestión, Corrupción y Seguridad Digital versión 6

La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo, clasificando su resultado en fuerte, moderado, débil como se indica.

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Riesgos de Gestión, Corrupción y Seguridad Digital versión 6

10.5.6 Nivel de riesgo (riesgo residual)

La mayoría de los controles que se diseñan son para disminuir la probabilidad de que ocurra una causa o evento que pueda llevar a la materialización del riesgo y muy pocos son dirigidos al impacto. Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo. Así mismo, y teniendo en cuenta que es un riesgo de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

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

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

Solidez del conjunto de los controles.	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir Impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la Probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de Impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No Disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No Disminuye	1	0
Moderado	No disminuye	Directamente	0	1

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Riesgos de Gestión, Corrupción y Seguridad Digital versión 6

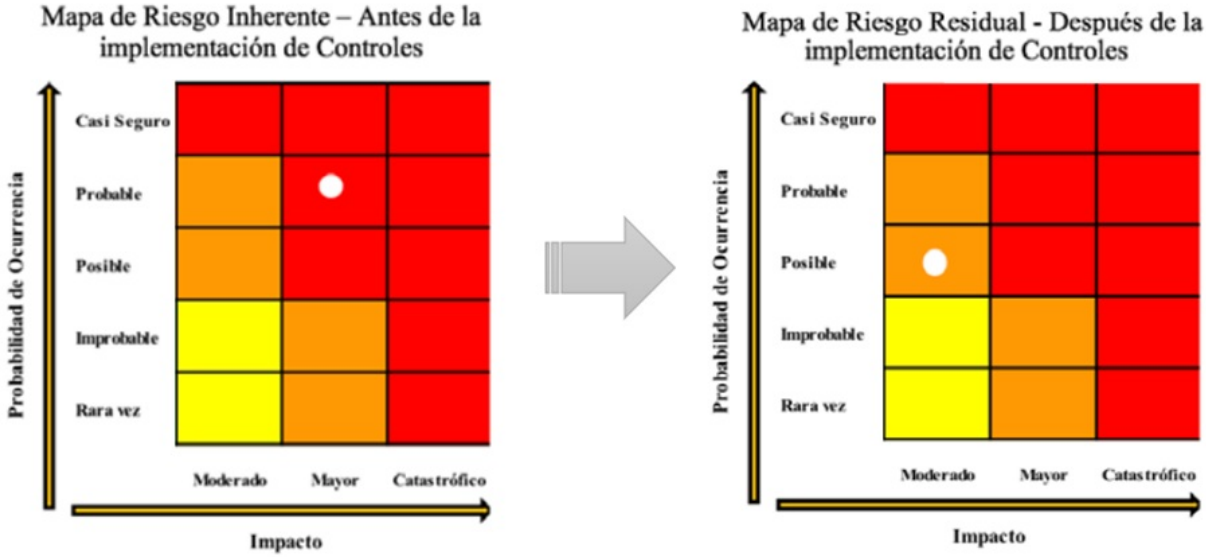
Inicialmente la Determinación de Ejecución del Control será una confirmación por parte del responsable del proceso, y posteriormente se debe ratificar con el cargue de las evidencias de las actividades de control en los periodos de corte establecidos dentro de la presente Política, de lo cual el Profesional de la Administración de Riesgos de la Oficina Asesora de Planeación elaborará un Informe de Seguimiento al vencimiento de cada periodo que a su vez la Oficina de Control Interno podrá realizar dentro de la Auditoría Interna (auditoría, evaluación o seguimiento) de acuerdo al Plan Anual de Auditoría – PPA aprobado o modificado por el Comité Institucional de Control Interno - CICCI.

Continuando con los criterios de Evaluación del Control, se establecerá la calificación de la ejecución del control con base en la siguiente tabla:

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

Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas. Versión 6

Con lo anterior se determina la posición del riesgo después de la ejecución del (los) control(es) considerando que están correctamente diseñados y que en efecto estos mitigan las causas, evitando que el riesgo se materialice. El desplazamiento en el Mapa de Calor debe ser similar al representado a continuación, siempre propendiendo una disminución en la Zona de Riesgo.



Fuente: Elaboración Propia

10.5.7 Tratamiento del riesgo

Dada la Zona de Riesgo Residual obtenida con la ejecución de controles, se realiza un tratamiento a los riesgos identificados que se aplica de la siguiente forma:

Reducir el riesgo: Se logra por medio de la implementación de controles adicionales que deberán analizarse dentro de un periodo de tiempo, cuyo limite es la finalización del Año que se encuentre en curso y dependiendo del resultado deberán incluirse como Controles para el siguiente Año.

Evitar el riesgo: Se elimina la ejecución de las actividades que facilitan la materialización del riesgo.

Compartir el riesgo: Se busca disminuir el impacto y/o la probabilidad del riesgo compartiéndolo con otro proceso de la Entidad o con un tercero actor, por ejemplo, mediante una póliza de seguro con una compañía exógena a la Entidad que deberán analizarse dentro de un periodo de tiempo, cuyo limite es la finalización del año que se encuentre en curso y dependiendo del resultado deberán incluirse como Controles para el siguiente año.

Todos los riesgos deben contar con algún tratamiento residual independiente de la Zona de Riesgo, únicamente están permitidas las actividades anteriormente descritas.

Se aclara que no existe zona de Riesgo residual Bajo, de tal forma todos los Riesgos deben contar con un Tratamiento diferente a Aceptar el Riesgo.

10.5.8 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 de Administración del Riesgo y evaluar su eficacia en el marco del desarrollo del Comité Institucional de Coordinación de Control Interno - CICCI.

Responsable	Riesgos de Gestión
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 10° día hábil una vez terminado el trimestre 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.
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 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 (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

10.5.9 Materialización de riesgos

Considerando la posibilidad materialización de un riesgo, es fundamental contar con una clara orientación sobre cómo actuar en caso de que esto ocurra. Las siguientes son las acciones que se deben seguir la primera línea de defensa en caso de materialización.

TIPO DE RIESGO	ACCIONES
Riesgos de Corrupción	Informar a la segunda y tercera línea de defensa de la materialización del riesgo y generar alerta de las posibles consecuencias.
	Identificar y ejecutar las acciones correctivas documentándolo en el plan de mejoramiento 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.

10.5.10 SARLAFT

La Superintendencia de Transporte atiende el llamado del gobierno nacional y afronta las medidas necesarias para evitar verse inmersa en eventos asociados al Lavado de Activos y la Financiación del Terrorismo por lo cual implementa el Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo SARLAFT, los riesgos que se detecten por la ejecución de dicha gestión son tratados íntegramente con la metodología impartida para los riesgos de Corrupción en la misma herramienta de seguimiento, monitoreo y evaluación.

La metodología y Política SARLAFT se imparten en documento independiente a la presente Política de Riesgos de la Entidad.

10.6. Riesgos Fiscales

Partiendo de la "*Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas*" el presente numeral tiene como finalidad prevenir el daño al patrimonio público, representando menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

Recordando que la responsabilidad fiscal está consignada en la Ley 610 de 2000. Las cuales 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 de defensa 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*", en el cual surge de los daños que se generaría sobre los recursos públicos, los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial, este último corresponde a los hechos inciertos o incertidumbres, con una potencial acción u omisión que podrían generar daño sobre los recursos públicos, los bienes y/o intereses patrimoniales de naturaleza pública; también se entiende el evento potencial como la causa raíz del Riesgo.

Para cumplir satisfactoriamente con el objetivo de la correcta administración del riesgo, se hace necesario seguir las siguientes etapas detalladamente. Se enfatiza en el objetivo de identificar, analizar, dar tratamiento, finalizando con el seguimiento y evaluación a los riesgos, logrando una visión integral de las actividades propias de la Entidad que podrían afectar el cumplimiento de las metas y objetivos trazados.

10.6.1 Etapa 1: Definición de niveles de aceptación del riesgo

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.2 Etapa 1. Definición de niveles de aceptación del riesgo*" del presente documento.

10.6.2 Etapa 2: Identificación del Riesgo

Para la identificación del riesgo fiscal es necesario establecer los puntos de Riesgo Fiscal que corresponde a las situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.
Lo anterior indica que son todas las actividades que representan la Gestión Fiscal, contemplando aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Complementando el ejercicio de los puntos de Riesgo se deben identificar las circunstancias inmediatas, siendo aquellas situaciones o actividades bajo la cual se presenta el riesgo, estas 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.

10.6.2.1 Identificación de Puntos de Riesgo Fiscales y Causa Inmediata

Para lograr una adecuada estructuración se desarrolla el siguiente ejercicio:

- Taller de Identificación: Realización de taller con los lideres 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 el taller, se formulan las siguientes preguntas:
    - ¿En qué procesos de la Entidad se realiza gestión fiscal?
    - ¿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 Oficina de Control Interno, en los últimos 5 años?
- Análisis del Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas: La Función Pública estructuró el "*CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS*" el cual suministra como Anexo 1 de la "*Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas*" en su versión 6, a continuación, se enuncian los puntos de Riesgo y las Circunstancias (Causas) inmediatas. Que pueden generar un efecto al patrimonio Público.

Id	Puntos de Riesgo Fiscal *Actividad en la que potencialmente se origina el riesgo fiscal*	Causa 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.
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, diseños recibidos, 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 asignarse 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).
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, no funcionales 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.	No funcionalidad 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.
39	Actas de liquidación suscritas.	Suscripción de acta de liquidación sin relacionar las sanciones impuestas a los contratistas
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: Anexo 1: Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas, Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas. Versión 6

Los ejercicios antes descritos deben efectuarse como mínimo una vez al año y deben respaldarse con Actas de reunión con los Lideres de Procesos y Operativos.

El ejercicio se respalda con la verificación de la matriz del Plan de mejoramiento de Contraloría de la Entidad y la asesoría de la Oficina de Control Interno.

10.6.2.2 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.

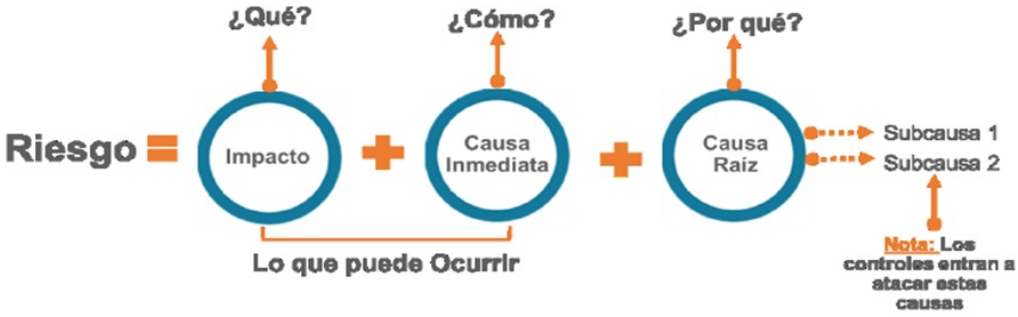
10.6.3 Etapa 3: Estructuración del riesgo Fiscal

Como parte fundamental en la Gestión del Riesgo, este se debe formular y redactar adecuadamente para lograr un entendimiento y tratamiento pertinente.

Para redactar un riesgo fiscal se debe tener en cuenta:

¿ Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
¿ Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
¿ 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:



Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas. Versión 6

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.

La redacción siempre debe iniciar con la frase POSIBILIDAD DE. De acuerdo con lo anterior, todos los Riesgos deben redactarse con la siguiente estructura:

Fuente: Elaboración Profesional Oficina Asesora de Planeación

Los siguientes son ejemplos de Riesgos Fiscales.

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 aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	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 no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista

Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas. Versión 6

10.6.4 Etapa 4. Valoración del Riesgo

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.2 Etapa 3. Valoración del Riesgo*" del presente documento.

10.6.5 Tratamiento del riesgo Inherente

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.3 Tratamiento del riesgo Inherentes*" del presente documento.

10.6.6 Ubicación en Mapa de Calor

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.4 Ubicación en Mapa de Calor*" del presente documento.

10.6.7 Valoración de Controles

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.5 Valoración de Controles*" del presente documento.

10.6.8 Análisis y evaluación del control

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.6 Análisis y evaluación del control*" del presente documento.

10.6.9 Nivel de riesgo residual

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.7 Nivel de riesgo residual*" del presente documento.

10.6.10 Estrategias para combatir el riesgo residual

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.8 Estrategias para combatir el riesgo residual*" del presente documento.

10.6.11 Monitoreo y seguimiento

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.9 Monitoreo y seguimiento*" del presente documento.

10.6.12 Materialización de riesgos

Para el riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el Numeral "*10.4.10 Materialización de riesgos*" del presente documento.

10.7 Riesgos de Seguridad de la Información

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.

Además, en la sección "*5.3. VALORACIÓN DEL RIESGO*", se resalta que la valoración de los riesgos se realiza siguiendo el lineamiento establecido para los riesgos de gestión. A partir del numeral "*10.4.2 Etapa 3. Valoración del Riesgo*" en adelante, se adoptan los numerales específicos para los riesgos de seguridad digital.

10.7.1 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 "7. 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 de Administración del Riesgo 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.

Responsable	Riesgos de Gestión
Primera línea de defensa (líderes de procesos, Enlace 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 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.
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 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

10.7.2 Materialización de riesgos

Considerando la posibilidad materialización de un riesgo, es fundamental contar con una clara orientación sobre cómo actuar en caso de que esto ocurra. Las siguientes son las acciones que debe seguir la Primera línea de defensa 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 mejoramiento fundamentado en el mapa de riesgos.
	Realizar seguimiento mensual para medir la efectivad 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 Oficina Asesora de Planeación – OAP y la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

10.8 Vigencia

Esta Política Institucional de Administración del Riesgo es aprobada por el Comité Institucional de Coordinación de Control Interno - CICCI.

Control de cambios		
Versión	**Fecha**	**Descripción del cambio**
1	Mayo 2016	Versión inicial del documento. Se definen los lineamientos para la Gestión del Riesgo en la Superintendencia de Transporte
2	Julio 2018	Se modifica la Política de Gestión del Riesgo, de acuerdo con los lineamientos de la Guía para administración del riesgo del Departamento Administrativo de la Función pública V3 de diciembre de 2014 y la Guía para la Gestión del Riesgo de Corrupción de la Secretaria de Transparencia – 2015
3	01-Sep-2019	Se modifica la Política de Administración del Riesgo, de acuerdo con los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 – octubre de 2018. Se incluye la gestión de riesgos de seguridad digital, para la Superintendencia de Transporte y los lineamientos del Decreto 2409 de 2018 Política que fue adoptada mediante Resolución Número 12263 del 7 de noviembre de 2019
4	16-Sep-2021	Se actualiza la Política de Administración del Riesgo, de acuerdo con los lineamientos de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas V5 – diciembre de 2020. Esta política se adoptó mediante Resolución Número 10867 del 5 de octubre de 2021.
005	2023-12-12 2023	Se actualiza la Política de Administración del Riesgo, de acuerdo con los lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V6 – diciembre de 2022 y su Versión 4 de 2018 Otorgando mayor precisión y claridad en todos los numerales que componen la Política

Aprobación del documento		
Etapa	**Nombre**	**Cargo**
Elaboró	Pablo Leonardo Molano Parra Jorge Nicolas Olaya Mesa	Contratista OAP Contratista OAP
Revisó	Juan David Benjumea Quintero	Jefe Oficina Asesora Planeación (E)
Aprobó	**Comité Institucional de Coordinación de Control Interno - CICCI**	

Juan David Benjumea Quintero @ 2024-01-09, 16:08:35