MANUAL PARA LA ADMINISTRACION DE LOS RIESGOS

Versión:
Unidad de Planeación de Infraestructura de Transporte
Grupo Interno de Trabajo de Planeación
Bogotá D.C., Julio 2024

TABLA DE CONTENIDO

Contenido

1. Introducción

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden ocasionar el incumplimiento de los objetivos que se han trazado; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de estos riesgos.

La administración de los riesgos es una herramienta fundamental para que las entidades puedan prevenir y gestionar aquellos eventos indeseables que pueden ocasionar el incumplimiento de sus objetivos institucionales.

El Modelo Integrado de Planeación y Gestión – MIPG contempla dentro de la Política de Planeación Institucional, como uno de sus lineamientos generales para su implementación, la necesidad que tienen las entidades del sector público de emitir las directrices precisas para administrar sus riesgos y definir lineamientos precisos para su tratamiento, manejo y seguimiento.

El Departamento Administrativo de la función Pública – DAFP, emitió la **Guía para la administración del riesgo y el diseño de controles en entidades públicas** como documento que permite facilitar la implementación de la Política de Riesgo de las entidades y unificar las metodologías existentes con el fin de hacer más sencilla la utilización de esta herramienta a través de un método lógico y sistemático que está compuesto de varios pasos, los cuales al ser ejecutados de manera periódica y secuencial facilitan la mejora continua en el proceso de toma de decisiones.

El Grupo Interno de Trabajo de Planeación elaboró el presente documento definiendo los elementos para efectuar una adecuada administración de riesgos en la Unidad de Planeación de Infraestructura de Transporte (en adelante UPIT).

2. ¿Para qué debo aplicar el documento?

Establecer los lineamientos metodológicos que permita a la UPIT a través de un método lógico y sistemático, administrar sus riesgos y gestionarlos a un nivel aceptable que le permita tener una seguridad razonable del logro de sus objetivos institucionales.

3. ¿Cuál es la aplicación del documento?

El manual para la administración del riesgo aplica para todos los procesos que conforman el mapa de procesos de la UPIT. Inicia con el análisis de la entidad y su horizonte estratégico y termina con los lineamientos para el monitoreo, seguimiento y evaluación de los mapas de riesgos.

El manual desarrolla los lineamientos para la administración de los riesgos de gestión, corrupción, seguridad de la información y fiscal.

4. ¿Qué conceptos debo tener claros para comprender el documento?

Definiciones:

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

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

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: a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc. b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas 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 (Causa Inmediata, pero se asocia a la misma causa inmediata)

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

Causa Raíz (Causa Eficiente o Causa Adecuada): Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.

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

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

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

Factores de Riesgo: Son las fuentes generadoras de riesgos.

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

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

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo

sustituya o modifique)4 ” . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista

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

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

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

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

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

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).

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.

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

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

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 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.

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

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

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

Siglas:

CICCI: Comité Institucional de Coordinación de Control Interno
CIGD: Comité Institucional de Gestión y Desempeño
MIPG: Modelo Integrado de Planeación y Gestión
UPIT: Unidad de Planeación de Infraestructura de Transporte

5. ¿Qué normatividad afecta el documento? (obligatorio)

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

6. ¿Qué documentos externos requiero en la ejecución?

Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 5 marzo 2023 – Departamento Administrativo de la Función Pública Función Pública – DAFP.

Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 noviembre de 2022 – Departamento Administrativo de la Función Pública Función Pública – DAFP.

7. ¿Qué documentos internos requiero en la ejecución

La documentación interna que hace parte de este manual se encuentra definidas en el Banco de Documentos de la UPIT, en el siguiente enlace: **Banco de Documentos**

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

Administrar adecuadamente los riesgos en la UPIT, requiere del compromiso y la resuelta participación de los directivos, funcionarios y contratistas; por esto, a continuación, se identifican los actores que intervienen y sus roles, de acuerdo con las directrices del Departamento Administrativo de la Función Pública, y el Modelo Integrado de Planeación y Gestión, tomando como base la estructuración de las líneas de defensa:

8.1. Línea Estratégica – Alta Dirección

Con el fin de garantizar una operación articulada y una adecuada gestión de los riesgos, La UPIT cuenta con el Comité Institucional de Gestión y Desempeño reglamentado a través de la Resolución 063 de 2022 y modificado por la Resolución 049 de 2023, el cual es el encargado de orientar la implementación y operación del Modelo Integrado de Gestión y Desempeño. Adicionalmente se ha creado el Comité Institucional de Coordinación de Control Interno reglamentado a través de la Resolución 096 de 2022.

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

COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO

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

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

- Revisar y aprobar el contexto estratégico, la plataforma estratégica, el modelo de operación por procesos y la planeación institucional, con el propósito de identificar cambios que puedan originar nuevos riesgos o modificar los existentes.
- Revisar y posicionar la Política de Administración del Riesgo de la Entidad.
- Revisar la información de cumplimiento de los objetivos institucionales y de los diferentes procesos, relativa a la implementación de la gestión de riesgos.
- Analizar el informe de evaluación a la gestión de riesgos y de ser necesario, proponer acciones para mejorar los planes para el tratamiento de estos.
- Establecer las políticas de operación encaminadas a controlar los riesgos que pueden llegar a incidir en el cumplimiento de los objetivos institucionales y verificar su cumplimiento.
- Analizar las evaluaciones de la gestión del riesgo, elaboradas por la Segunda y Tercera Línea de Defensa

COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO

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

Así mismo le corresponde:

- Evaluar y dar lineamientos técnicos sobre la administración de los riesgos de la Entidad
- Retroalimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo, la aplicación de los controles y realización de las acciones formuladas por el proceso para el fortalecimiento de estos.
- Evaluar la aplicación de las acciones de contingencia en los casos en que se presenta la materialización de un riesgo

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

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

LÍDERES DE PROCESOS

Los líderes de proceso tienen la responsabilidad de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se divulguen a cada servidor

público y/o contratista que trabaja en el proceso, es importante recordar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

Adicionalmente, la primera línea debe:

- Evaluar los cambios que se presenten en la plataforma estratégica de la entidad o en su contexto estratégico, analizando cómo estos cambios originan nuevos riesgos o modifican los ya existentes.
- Liderar la identificación de los riesgos del proceso a cargo, siguiendo los lineamientos establecidos en el Manual de Administración del Riesgo de la UPIT
- Realizar, con el apoyo de su grupo de trabajo, la gestión y administración de los riesgos identificados.
- Realizar la evaluación de la formulación y la solidez de los controles, para determinar la pertinencia y la necesidad de ajuste o modificación, en caso de presentarse.
- Adelantar la revisión, actualización periódica y seguimiento de los mapas de riesgos, y si es el caso ajustarlos.
- Establecer controles que contribuyan a mitigar riesgos del proceso.
- Socializar los controles implementados con su equipo de trabajo, con el fin de asegurar que sean comprendidos por todos, garantizando su correcta y oportuna aplicación.
- Monitorear constantemente la correcta aplicación de los controles
- Analizar los eventos de materialización de los riesgos y aplicar los lineamientos que se definan para su adecuada gestión.

FUNCIONARIOS Y CONTRATISTAS

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

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

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

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

ASESORÍA GESTIÓN TIC– PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

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

8.4. Tercera Línea –Asesor Control Interno

- Establecer el plan anual de auditoría basado en riesgos, priorizando aquellos procesos de mayor exposición, así como la verificación del funcionamiento de los componentes de control interno

- Evaluar la efectividad de la Gestión del Riesgo en la Entidad a través de la verificación de la adecuado diseño y aplicación de controles y su aporte en la mitigación de los riesgos identificados.

- Adelantar el registro de no conformidades, en el marco de las auditorías internas, cuando se constituya un incumplimiento en la aplicación de la política de riesgo.

- Acompañar y asesorar metodológicamente a los procesos, en la administración y gestión integral de riesgos, en coordinación con la segunda línea de defensa.

- Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.

- Comunicar al Comité de Coordinación de Control Interno posibles cambios evidenciados en la evaluación del riesgo, detectados durante las auditorías.

- Alertar a la alta dirección sobre la probabilidad de riesgo de corrupción en las áreas auditadas.

9. Políticas de Operación para la Administración del Riesgo

Con el fin de contar con una herramienta útil que le permita a la UPIT un aseguramiento razonable con respecto al logro de los objetivos, a continuación, se establecen los lineamientos que se deben tener en cuenta en la Unidad para la administración del riesgo.

- Por lo menos una vez al año, cada proceso debe construir, revisar y/o modificar sus Mapas de Riesgos de gestión y corrupción.

- Le corresponde a la segunda línea de defensa el análisis de los objetivos de la entidad, tanto del orden estratégico como de procesos.

- La identificación de los riesgos en la UPIT se realizará teniendo en cuenta los objetivos de los procesos que a su vez deben estar alineados con los objetivos estratégicos de la Entidad.

- La consolidación del mapa de Riesgos estará a cargo del Grupo Interno de Trabajo de Planeación

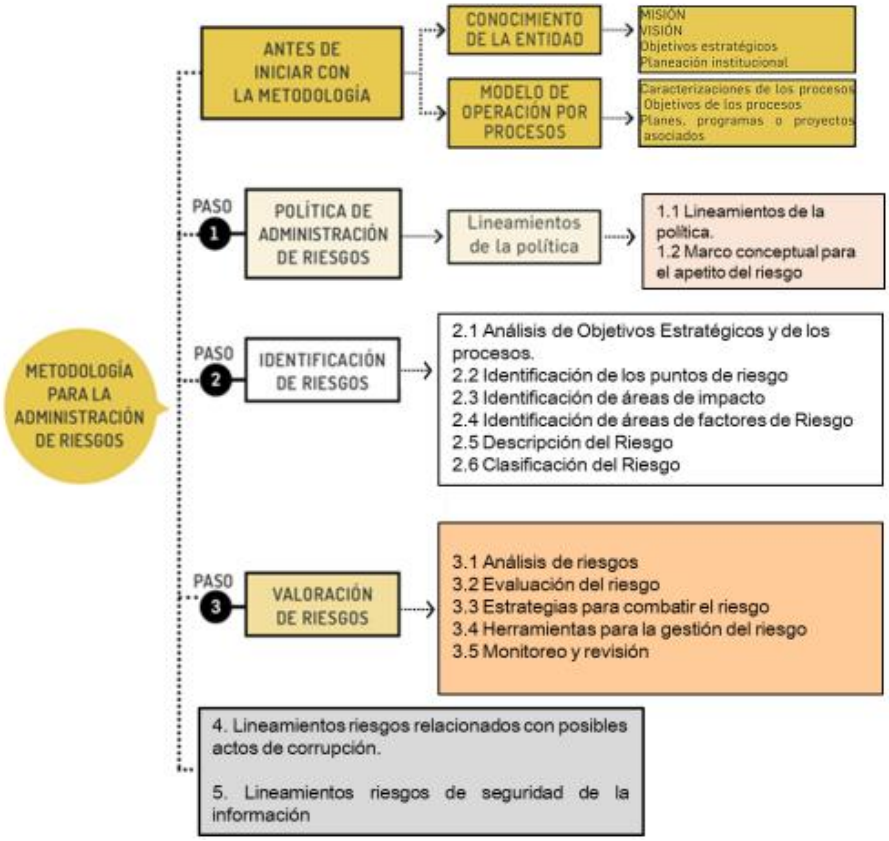
- El Grupo Interno de Trabajo Planeación solicitará la publicación del mapa de riesgos de corrupción en la página web de la entidad a más tardar el 31 de enero de cada año cumpliendo lo establecido en el Decreto 1081 de 2015

- Tras la materialización de un riesgo, el líder del proceso, con el acompañamiento del Grupo Interno de Trabajo Planeación, debe analizar la situación presentada, identificar los controles que fallaron y realizar los ajustes a los que haya lugar. Adicionalmente se debe evaluar nuevamente el riesgo en su probabilidad e impacto y registrar la información de lo ocurrido en la matriz "base histórica de eventos"

10. Metodología para la Administración del Riesgo

10.1. Acerca de la Metodología

Antes de empezar con la



implementación de la metodología, es necesario conocer la entidad desde un punto de vista estratégico para posteriormente avanzar en el desarrollo de los tres (3) pasos básicos que permitan generar la estructura para la administración de los riesgos a la UPIT

Metodología para la Administración del Riesgo

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 – DAFP

10.2. Antes de Iniciar

Es importante conocer cuál es el propósito de la entidad (Misión), sus aspiraciones para el futuro (Visión) y sus metas a largo plazo (Objetivos Estratégicos).

Por otra parte, también es importante conocer como es el modelo de operación por procesos de la Unidad, entendido como la estructura definida al interior de la UPIT para cumplir con las funciones otorgadas por la ley. En este punto es importante conocer la cadena de valor de la UPIT (Mapa de Procesos) y la caracterización de los procesos, herramienta que consolida el objetivo del proceso y las principales actividades desarrolladas al interior de este.

10.3. Paso 1. Política de Administración del Riesgo

La política de administración del riesgo es la declaración e intención general que hace la UPIT respecto a la gestión y administración de sus riesgos, estableciendo lineamientos precisos para su tratamiento, manejo y seguimiento.

"*La Unidad de Planeación de Infraestructura de transporte – UPIT gestionará sus riesgos con base en los lineamientos establecidos en el presente documento, buscando así evitar y/o mitigar las consecuencias en caso de materialización, mediante actividades de prevención, sensibilización y control buscando garantizar de manera razonable el cumplimiento de sus objetivos institucionales*"

10.3.1. Niveles de tolerancia del riesgo en la UPIT

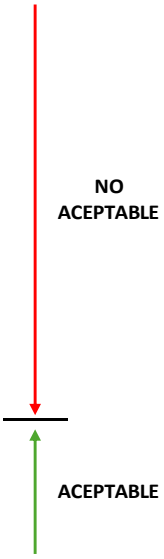
Entendiendo que la administración de los riesgos es un ejercicio dinámico que en la Unidad se ira desarrollando en la medida que se implemente la herramienta y se desarrolle la metodología, se establecen los siguientes niveles de aceptación para los riesgos, relacionados con las diferentes zonas del mapa de calor adoptado en la UPIT.

Apetito / Aceptación del riesgo: Entendido como el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. En la UPIT se podrán aceptar aquellos riesgos que se ubiquen en el nivel de riesgo bajo, identificado por el color verde dentro del mapa de calor.

Tolerancia del riesgo: Entendido como el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor de aceptación del riesgo determinado por la entidad. En la UPIT, cada nivel de tolerancia conlleva el desarrollo de acciones con diferentes prioridades y en horizontes de tiempo diversos.

Matriz de Tolerancia del riesgo en la UPIT

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



10.4. Paso 2. Identificación de Riesgos

Este paso tiene como objetivo, identificar los riesgos que estén o no bajo el control de la Entidad, para ello se debe tener en cuenta el contexto estratégico en el que opera la UPIT, la caracterización de cada proceso que contempla su objetivo y alcance y también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Para identificar los riesgos, es necesario desarrollar las siguientes fases:

10.4.1. Análisis de objetivos estratégicos y de procesos

Objetivos Estratégicos

Es necesario que se haga la revisión de los objetivos estratégicos definidos por la UPIT para garantizar que éstos cumplan con las características mínimas de ser específicos, medibles, alcanzables, relevantes y proyectados en el tiempo, así mismo se debe verificar que se encuentren alineados con la Misión y la Visión Institucional.

Una vez realizada la revisión anterior, se procede a identificar aquellas situaciones potenciales que, de llegar a ocurrir, afectaría su cumplimiento de los objetivos

institucionales.

Objetivos de Procesos

De igual manera, se deben analizar los objetivos de los procesos con base en las mismas características explicadas para los objetivos estratégicos, esto es, frente a las características de su redacción y su alineación con la misión y la visión, buscando asegurar que contribuyan al logro de los objetivos estratégicos

Características de Objetivos SMART

10.4.2. Identificación de los puntos de riesgos

Los puntos de riesgos son aquellas actividades del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo que deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Para identificar los puntos de riesgos, el proceso puede:

- Revisar el objetivo del proceso e identificar los verbos que denotan las principales acciones que el proceso desarrolla
- Revisar en su caracterización, las principales actividades desarrolladas por el proceso para transformar los insumos en productos

10.4.3. Identificación de las áreas de impacto

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

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

10.4.4. Factores de Riesgos

Los factores de riesgo, en términos generales, hacen referencia a las fuentes en donde se pueden originar riesgos, es decir; aquellos aspectos dentro o fuera de la entidad que podrían generar eventos que terminen en el incumplimiento de los objetivos institucionales o de los procesos

En la UPIT los eventos o riesgos pueden ser generados por los siguientes factores:

FACTOR	DEFINICIÓN	DESCRIPCIÓN
PROCESOS	Eventos relacionados con errores en las actividades que deben realizar los servidores de la Unidad, falta de documentación de actividades o incumplimiento de las actividades establecidas	Falta de Procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos o externos
		Falta de capacitación, aspectos relacionados con los servidores
TALENTO HUMANO	Incluye seguridad y salud en el trabajo, también se debe analizar posible dolo e intención frente a la corrupción	Hurto de Activos
		Posibles comportamientos no éticos de los servidores
		Fraude Interno (corrupción, soborno)
TECNOLOGÍA	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de Equipos
		Caída de Aplicaciones
		Caída de Redes
		Errores en programas
		Hackeo de los sistemas de la entidad
		Afectaciones a la confidencialidad, integridad o disponibilidad de los activos de información de la UPIT
INFRAESTRUCTURA	Eventos relacionados con la infraestructura física de la entidad	Derrumbes
		Incendios
		Inundaciones
		Daños a activos físicos
		Falta de mantenimiento
EVENTOS EXTERNOS	Situaciones externas que afectan a la entidad	Suplantación de Identidad
		Temas relacionados con inseguridad en la ciudad
		Atentados, vandalismo, situaciones relacionadas con el orden público
		Incumplimientos o cambio en los requisitos para la operación de las unidades

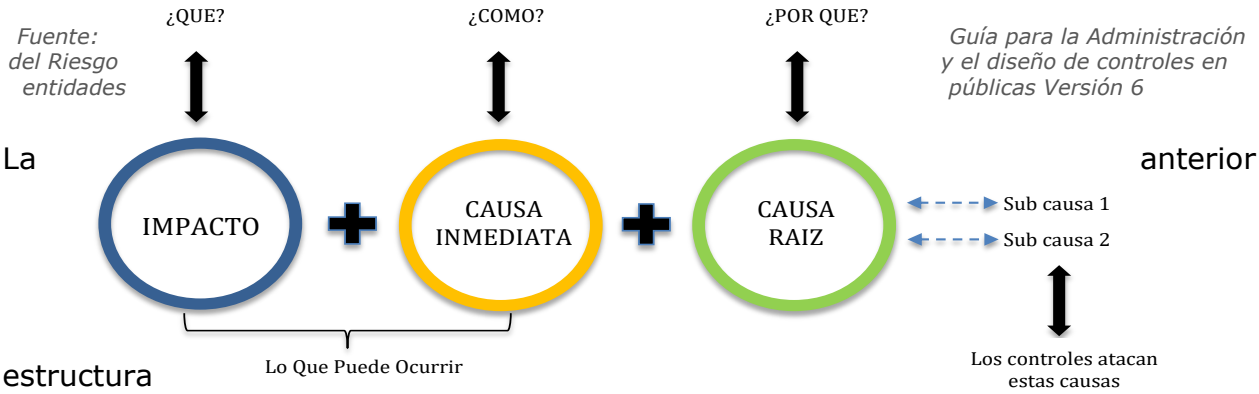
Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Nota: Estos factores de riesgo pueden variar, se sugiere analizar anualmente para determinar la necesidad de incluir o eliminar factores de acuerdo con la dinámica de la entidad

10.4.5. Descripción de Riesgos

La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea fácil de entender tanto para las personas que hacen parte del proceso como para personas ajenas al mismo.

Se propone la siguiente estructura buscando facilitar su redacción y claridad, iniciando siempre con la frase *POSIBILIDAD DE…* y analizando los siguientes aspectos:



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

La anterior estructura busca evitar la subjetividad al momento de redactar 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.

Desglosando la estructura propuesta tenemos:

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

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

Causa raíz: 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. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o sub-causas que pueden ser analizadas.

Ejemplo:

Proceso: Gestión Contractual

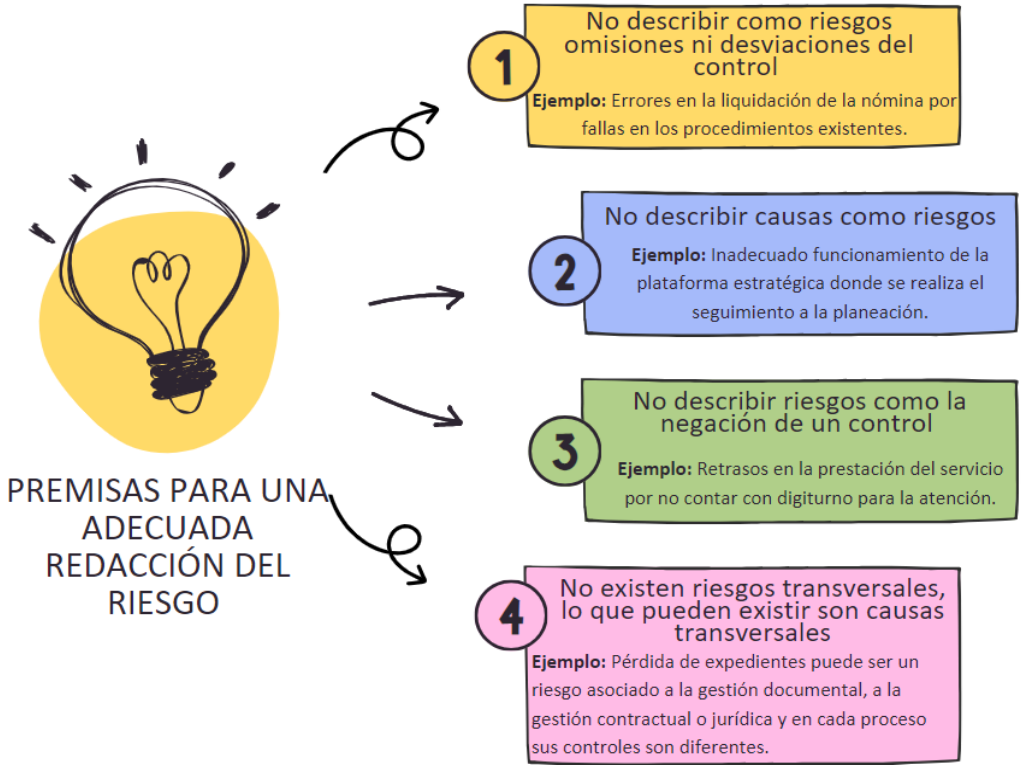
Objetivo: Gestionar, mediante el desarrollo de las modalidades de selección contractual, la adquisición de los bienes y servicios requeridos por la entidad para atender las necesidades previstas en el Plan Anual de Adquisiciones en cumplimiento de su misionalidad y de su funcionamiento. Todo de acuerdo con el Manual de contratación y la normatividad vigente.

Alcance: Inicia con la solicitud de contratación de las áreas que generan la necesidad, previa estructuración técnica del proceso y verificación del PAA y culmina con la liquidación y/o acta de cierre contractual según corresponda.

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

Inicio de la redacción	¿Que?	¿Como?	¿Por qué?
Posibilidad de…	*afectación económica*	*por sanciones de entes de control en los procesos de contratación*	*debido a una equivocada Identificación de la modalidad contractual al momento de definirla en el Plan Anual de Adquisiciones.*
	Impacto	**Causa Inmediata**	**Causa Raíz**

Premisas para una adecuada redacción del riesgo



10.4.6. Clasificación de los Riesgos

Busca clasificar los riesgos identificados en alguna de las siguientes categorías:

Clasificación del Riesgo	Descripción
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos y sus procedimientos
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.

Clasificación del Riesgo	Descripción
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 06

La utilidad de la clasificación de los riesgos está en poder articularla con los **factores generadores** que se determinaron en el numeral *10.4.4 Identificación de áreas de factores de riesgo* del presente documento a fin de orientar el tipo de controles que se deben definir para su mitigación

Su interrelación es la siguiente:

Relación ente factores de riesgo y clasificación del riesgo

CLASIFICACIÓN DEL RIESGO		FACTORES DE RIESGO
Ejecución y Administración de Procesos	→	Procesos
Fraude externo	→	Evento Externo
Fraude interno	→	Talento Humano
Fallas tecnológicas	→	Tecnología
Relaciones laborales	→	Pueden asociarse a varios factores
Usuarios, productos y prácticas	→	
Daños a activos fijos	→	Infraestructura
	→	Evento Externo

10.5. Paso 3. Valoración del Riesgo

La valoración de los riesgos consiste en establecer la probabilidad de ocurrencia del evento identificado y el nivel de consecuencia o impacto que causaría la materialización de este. La relación entre estas dos variables se determina ***Zona de riesgo inicial***.

La valoración de los riesgos se desarrolla a partir de los siguientes elementos:

Análisis de riesgos: Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias, con el fin de estimar la zona de riesgo inicial o **Riesgo Inherente**

Evaluación de Riesgos: Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final **Riesgo Residual**

A continuación, se realiza la descripción de cada uno de los elementos que desarrollan la valoración del riesgo

10.5.1. Análisis de riesgos

En esta primera etapa se busca establecer la *probabilidad* de ocurrencia de los riesgos que el proceso o la Unidad ha identificado, así como el *impacto* que tendría una eventual materialización. Con este análisis se busca determinar el ***nivel del riesgo***, entendido como el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

10.5.1.1. Determinación de la probabilidad de ocurrencia de un riesgo

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

Con este esquema se busca que "*la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.*"[1]

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

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 NOVIEMBRE 2022

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 06

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

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

10.5.1.2. Determinación del Impacto de un riesgo

Tal como se identificó en el numeral 10.4.3 del presente manual; para la UPIT el impacto de la materialización de un riesgo será ***económico o reputacional.***

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

Para determinar el impacto que tendría en la Unidad la materialización de un riesgo, se utilizarán los criterios definidos en la siguiente tabla; es importante definir con claridad el área del impacto del riesgo, pues los criterios de cada área son diferentes:

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 06

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

Continuación del Ejemplo

Proceso: Gestión Contractual

Objetivo: Gestionar, mediante el desarrollo de las modalidades de selección contractual, la adquisición de los bienes y servicios requeridos por la entidad para atender las necesidades previstas en el Plan Anual de Adquisiciones en cumplimiento de su misionalidad y de su funcionamiento. Todo de acuerdo con el Manual de contratación y la normatividad vigente.

Riesgo Identificado: Posibilidad de pérdida reputacional por sanciones de entes de control en los procesos de contratación debido a una equivocada identificación de la modalidad contractual al momento de definirla en el Plan Anual de Adquisiciones.

No. de veces que se ejecuta la actividad (Probabilidad): la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año (También se podría tomar como referencia el No. De contratos de la vigencia anterior)

Cálculo afectación reputacional (Impacto): De llegar a materializarse, se estima que el riesgo afectaría la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos, es decir un impacto "Moderado"

Aplicando las tablas de probabilidad e impacto tenemos:

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

La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es **MEDIA**.

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

La afectación reputacional se encuentra en 60%, el impacto del riesgo sería MODERADO

Probabilidad Inherente= MEDIA 60%, **Impacto Inherente:** MODERADO 60%

10.5.2. Evaluación del riesgo

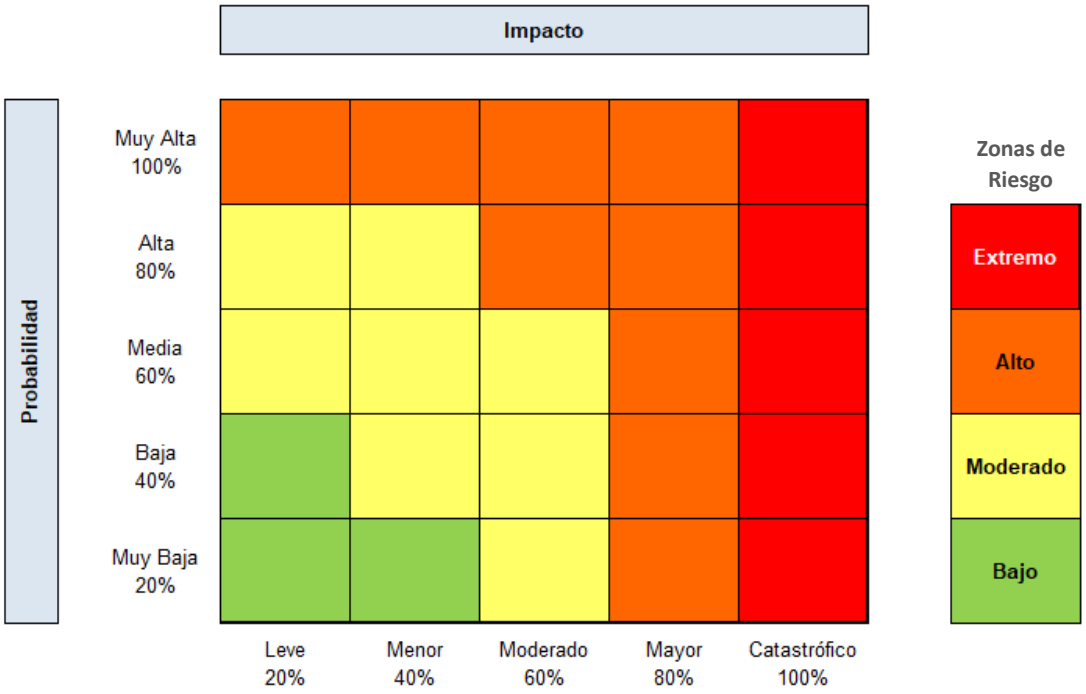
Una vez valorado el riesgo, es decir determinada la probabilidad y el impacto inherente del riesgo identificado, se procede a determinar la zona de riesgo inicial o ***Riesgo Inherente***.

10.5.2.1. Análisis Inicial

En esta etapa se busca determinar el nivel de severidad del riesgo a través de la combinación entre la probabilidad de ocurrencia del riesgo y su impacto en caso de una eventual materialización.

Para este ejercicio en la UPIT se utiliza un mapa de calor o matriz de calor de 5X5 es decir 5 niveles para la probabilidad y 5 niveles para el impacto.

Mapa de Calor



Continuación del Ejemplo

Proceso: Gestión Contractual

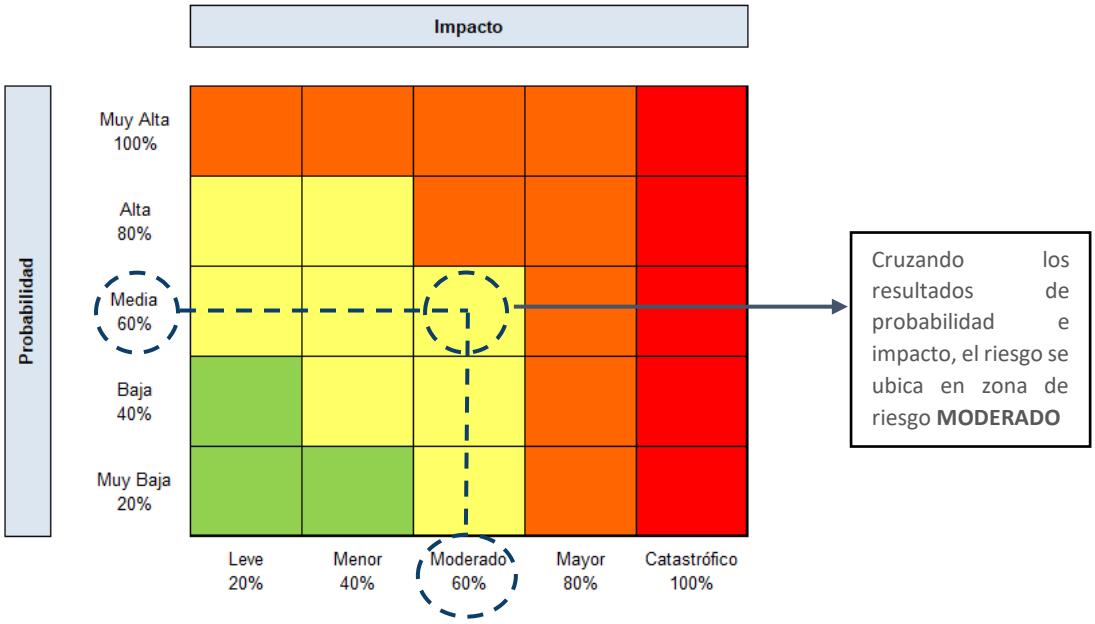
Objetivo: Gestionar, mediante el desarrollo de las modalidades de selección contractual, la adquisición de los bienes y servicios requeridos por la entidad para atender las necesidades previstas en el Plan Anual de Adquisiciones en cumplimiento de su misionalidad y de su funcionamiento. Todo según el Manual de contratación y la normatividad vigente.

Riesgo Identificado: Posibilidad de pérdida reputacional por sanciones de entes de control en los procesos de contratación debido a una equivocada identificación de la modalidad contractual al momento de definirla en el Plan Anual de Adquisiciones.

Probabilidad Inherente: MEDIA (60%)

Impacto Inherente: MODERADO (60%)

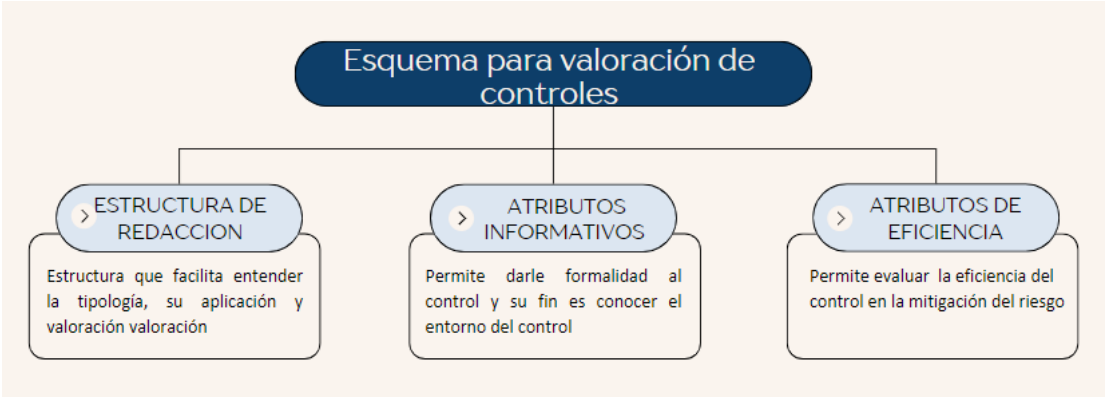
Aplicando los datos en el mapa de calor tenemos:



10.5.2.2. Valoración de los controles

Un control se puede definir como una *Medida que modifica el riesgo*[2]; los controles son actividades que el proceso desarrolla en su quehacer cotidiano y que, si se aplican sistemáticamente, se pueden convertir en medidas que ayudan a mitigar los riesgos.

Es necesario valorar los controles a fin de determinar su pertinencia en la mitigación de los riesgos, para lo cual se utilizará el siguiente esquema:



[2] NTC-ISO 31000

Elaboración propia con base en información de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 06

Estructura de Redacción

Para una adecuada redacción del control se propone una estructura que busca facilitar el entendimiento de la tipología del control y su correcta aplicación. La estructura es la siguiente:

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Frecuencia de Aplicación:** Determina la frecuencia con que debe aplicarse el control
- **Acción:** Se determina mediante verbos que indican la acción que deben realizar como parte del control. Por lo general, las acciones de control establecen actividades en donde se compara o verifica el cumplimiento de criterios previamente definidos; se identifican con verbos como: revisar, verificar, confrontar, comparar, cotejar, analizar etc.
- **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo de redacción de un control

Responsable	Frecuencia de Aplicación	Accion de Control	Complemento
Profesional de la Secretaría General	mensualmente	realiza acompañamiento en la estructuración de los estudios previos y estudios de mercado	verificando el cumplimiento de los requisitos establecidos en el Manual de Contratación. En caso de que los estudios no cumplan con lo establecido, realiza la devolución al proceso para que sean ajustados

Atributos Informativos

Los atributos informativos permiten darle formalidad al control, ayudan a garantizar su permanencia en el tiempo, así como su correcta aplicación. Su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Dentro de los atributos informativos tenemos:

- **Documentación**: Busca determinar si los controles definidos para mitigar el control se encuentran documentados ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.

- **Frecuencia de Aplicación**: Determina si el control definido tiene establecido la frecuencia con que debe aplicarse el control

- **Evidencia**: Busca establecer, si producto de la aplicación del control quedan registros que evidencien su ejecución.

Atributos de Eficiencia

Los atributos de eficiencia tienen incidencia directa en la efectividad que el control tiene en la mitigación del riesgo. Se dividen en dos; Atributos de tipo y atributos de implementación.

- Atributos de tipo: Busca determinar la orientación que tiene el control de acuerdo con las siguientes tipologías:

    - **Control preventivo**: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

    - **Control detectivo**: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

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

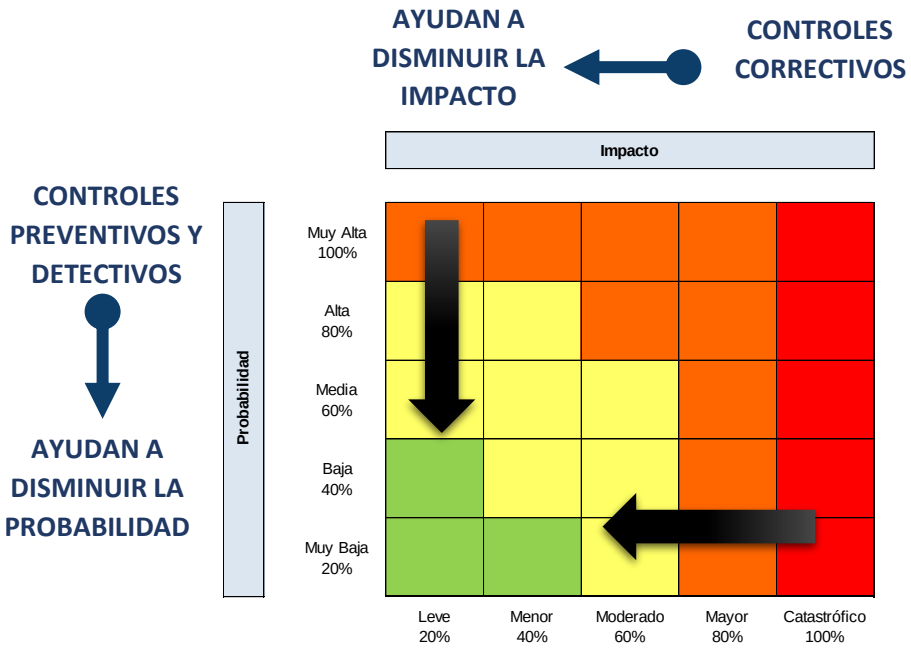
- Atributos de Implementación: Busca establecer si los controles definidos se ejecutan de forma manual o automática

10.5.2.3. Análisis y evaluación de los controles

Si bien, la estructura de redacción y los atributos informativos que se desarrollaron en el punto anterior son muy importantes al momento de redactar un control, estos no tienen una incidencia directa en su efectividad.
Por otra parte, los atributos de eficiencia inciden directamente en la efectividad del control; a continuación, se analizan estos atributos del control, para determinar en qué porcentaje el control puede ayudar a mitigar el riesgo.

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%

Esta calificación de los controles permite determinar el movimiento que tendrá el riesgo dentro del mapa de calor disminuyendo la probabilidad o el impacto; dependiendo del tipo de control que se tenga definido así:



Teniendo en cuenta el anterior diagrama, siempre será recomendable que los procesos definan controles de diferentes tipos, con el fin de asegurar una mitigación efectiva de los riesgos.

Continuación del Ejemplo

Proceso: Gestión Contractual

Objetivo: Gestionar, mediante el desarrollo de las modalidades de selección contractual, la adquisición de los bienes y servicios requeridos por la entidad para atender las necesidades previstas en el Plan Anual de Adquisiciones en cumplimiento de su misionalidad y de su funcionamiento. Todo de acuerdo con el Manual de contratación y la normatividad vigente.

Riesgo Identificado: Posibilidad de pérdida reputacional por sanciones de entes de control en los procesos de contratación debido a una equivocada identificación de la modalidad contractual al momento de definirla en el Plan Anual de Adquisiciones.

Probabilidad Inherente: MEDIA (60%)

Impacto Inherente: MODERADO (60%)

Zona de riesgo: MODERADO

Control 1: el profesional de la Secretaría General mensualmente realiza acompañamiento en la estructuración de los estudios previos y estudios de mercado verificando el cumplimiento de los requisitos establecidos en el Manual de Contratación. En caso de que los estudios no cumplan con lo establecido, realiza la devolución al proceso para que sean ajustados

Control 2: el jefe del área de contratos diariamente verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Evaluando los controles con los criterios establecidos en el numeral 10.5.2.3 tenemos:

Controles y Sus Caracteristicas				Peso
Control 1 el profesional de la Secretaría General mensualmente realiza acompañamiento en la estructuración de los estudios previos y estudios de mercado verificando el cumplimiento de los requisitos establecidos en el Manual de Contratación. En caso de que los estudios no cumplan con lo establecido, realiza la devolución al proceso para que sean ajustados	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automatico		
		Manual	X	15%
Total valoración control 1				**30%**
Control 2 el jefe del área de contratos diariamente verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automatico		
		Manual	X	15%
Total valoración control 2				**30%**

10.5.2.4. Determinación del Riesgo Residual

Por riesgo residual se entiende el riesgo resultante después de que se evalúen los controles y su efecto en la mitigación del riesgo.

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

Dando continuidad al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles y determinación del riesgo residual.

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de afectación económica por sanciones de entes de control en los procesos de contratación debido a una equivocada identificación de la modalidad contractual al momento de definirla en el Plan Anual de Adquisiciones.	Probabilidad inherente	60%	Valoración control 1 detectivo	30%	60%* 30% = 18% 60% - 18% = 42%
	Valor probabilidad para aplicar 2o control	42%	Valoración control 2 detectivo	30%	42%* 30% =12,6% 42% - 12,6% = 29,4%
	Probabilidad Residual				**29,40%**
	Impacto Inherente	60%	No se tienen controles para aplicar al impacto	N/A	N/A
	Impacto Residual				**60%**

Continuación del Ejemplo

Objetivo: Gestionar, mediante el desarrollo de las modalidades de selección contractual, la adquisición de los bienes y servicios requeridos por la entidad para atender las necesidades previstas en el Plan Anual de Adquisiciones en cumplimiento de su misionalidad y de su funcionamiento. Todo de acuerdo con el Manual de contratación y la normatividad vigente.

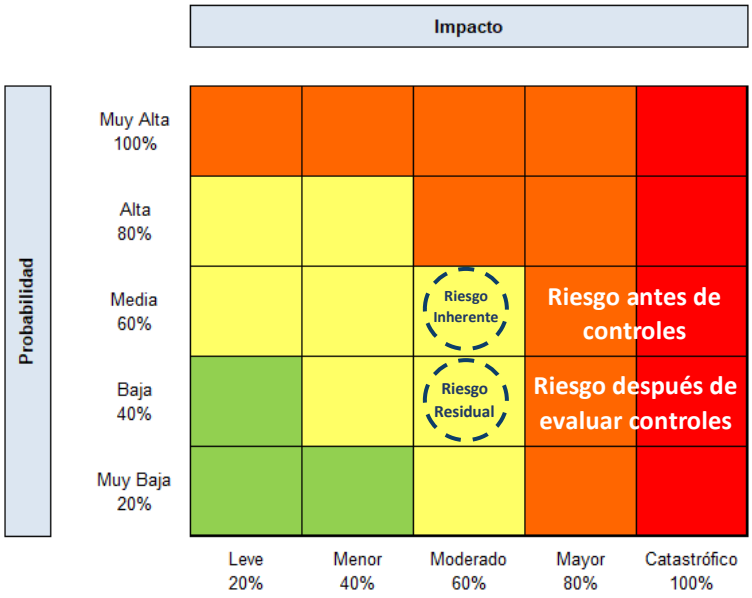
Riesgo Identificado: Posibilidad de pérdida reputacional por sanciones de entes de control en los procesos de contratación debido a una equivocada identificación de la modalidad contractual al momento de definirla en el Plan Anual de Adquisiciones.

Riesgo antes de controles		
Probabilidad Inherente:	MEDIA	60%
Impacto Inherente:	MODERADO	60%
Zona de riesgo:	MODERADO	

Riesgo despues de evaluar los controles		
Probabilidad Residual:	BAJA	29,4%
Impacto Residual	MODERADO	60%
Zona de riesgo:	MODERADO	

Para este ejemplo, si bien el riesgo se mantiene en zona MODERADO, disminuyo la probabilidad de su ocurrencia.

Dentro del mapa de calor, se observa el movimiento del riesgo de la siguiente manera:



Nota: Una buena administración de los riesgos busca llevarlos a la zona de riesgo BAJO, identificada con el color verde, por lo tanto, es recomendable identificar todos los controles necesarios para atacar tanto la probabilidad de ocurrencia como el impacto

10.5.3. Estrategias para combatir el riesgo

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

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

Si después de evaluar los controles definidos por el proceso para el riesgo aún permanece en zona de riesgo MODERADO, ALTO o EXTREMO, se sugiere una estrategia para ***Reducir el riesgo***, es decir; implementar acciones[3] que ayuden a fortalecer los controles (aumentar su calificación en la evaluación) o desarrollar

[3] Se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento, este plan es conocido como Plan de Tratamiento de Riesgos

acciones nuevas con el fin de evaluar si eventualmente pueden ser consideradas como nuevos controles que ayuden a disminuir la probabilidad o el impacto.

Las acciones definidas y los tiempos de su implementación dependerán de la zona de riesgo en donde se ubique el riesgo[4] (Ver la Matriz *de Tolerancia del riesgo en la UPIT* de la página 13 del presente documento). Es importante aclarar que el plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio[5] y se consideraría un control correctivo.

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

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

10.5.4. Herramientas para la gestión del riesgo

Además de los mapas de riesgo, se cuenta con otras herramientas que aportan información valiosa para la gestión de los riesgos, por ejemplo:

Gestión de eventos: Se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de ayuda
- Las PQRSD (peticiones, quejas, reclamos, sugerencias, denuncias)

[4] El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un control correctivo.

[5] De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

- Oficina Jurídica
- Líneas internas de denuncias

Estas herramientas generan información relacionada sobre posibles materializaciones de los riesgos.

Indicadores clave de riesgo: hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.
Algunos ejemplos de estos indicadores pueden ser:

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

10.5.5. Monitoreo y Revisión

En esta etapa se desarrollan los lineamientos para realizar el seguimiento periódico a la gestión de los riesgos identificados en la UPIT, mediante el monitoreo a la operación y aplicación adecuada de los controles, el avance en las acciones asociadas y en caso de la materialización del riesgo, la correcta aplicación de las acciones de control correctivas.

- **Monitoreo**

Cada cuatro meses, durante enero, mayo y septiembre y con corte al último día hábil de los meses de diciembre, abril, y agosto, los líderes de los procesos con el apoyo de su equipo de trabajo, deben realizar el monitoreo a la gestión de sus riesgos.

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

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

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

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

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

Lo anterior implica que se realice la valoración de los nuevos controles teniendo en cuenta lo establecido en el numeral *10.5.2.2 Valoración de los controles* del presente documento y medir como los nuevos controles contribuyen en la mitigación del riesgo aplicando los lineamientos establecidos en el numeral *10.5.2.3 Análisis y evaluación de los controles* y de acuerdo con la zona en donde quede ubicado el riesgo residual se determine las estrategias para combatir el riesgo para lo cual se puede remitir al numeral *10.5.3 Estrategias para combatir el riesgo*

Materialización del Riesgo: Se debe reportar si en el periodo evaluado, el riesgo se materializó o no. En caso de que en el periodo evaluado se presente la materialización de un riesgo, se debe reportar la aplicación de los controles correctivos definidos por el proceso con sus respectivas evidencias. Adicional a lo anterior, en caso de la materialización de un riesgo de corrupción el proceso debe demostrar, la puesta en conocimiento ante las autoridades o entes de control que regulan la gestión de la Unidad (Fiscalía, Contraloría General de la República, Procuraduría General de la Nación, Control Interno Disciplinario, etc.)

Tras la materialización de un riesgo, el proceso debe registrar la información de lo ocurrido en la matriz "**base histórica de eventos"** y realizar la revisión integral del riesgo y sus controles, con el fin de determinar cuál de ellos falló o no fue aplicado, causando la materialización del riesgo. Finalmente debe definir acciones encaminadas a fortalecer los controles existentes o a crear nuevos controles (Plan de Tratamiento del Riesgo) buscando evitar que se vuelva a presentar una materialización.

- **Seguimiento**

A partir de la información registrada por los líderes de los procesos frente al monitoreo de sus riesgos, el Grupo Interno de Trabajo – Planeación realizará seguimiento al estado de aplicación de la práctica, para lo cual revisará los avances reportados por los procesos en la aplicación de sus controles y en el desarrollo de sus acciones de fortalecimiento y analizará si las evidencias proporcionadas son coherentes con los avances presentados.

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

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

Tras la materialización de un riesgo, el Grupo Interno de Trabajo – Planeación debe velar por que el proceso registre la información de lo ocurrido en la matriz "base histórica de eventos", realice nuevamente la revisión y evaluación del riesgo y sus controles, así como la definición de acciones de fortalecimiento que busquen evitar que se vuelva a presentar una materialización

- **Evaluación**

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

FECHAS DE SEGUIMIENTO A LA ADMINISTRACIÓN DE LOS RIESGOS

SEGUIMIENTO	FECHA DE CORTE	FECHA DE REPORTE
Primer Seguimiento	30 de abril	Primeros cinco (5) días hábiles del mes de mayo
Segundo Seguimiento	31 de agosto	Primeros cinco (5) días hábiles del mes septiembre
Tercer Seguimiento	31 de diciembre	Primeros cinco (5) días hábiles del mes enero

El monitoreo y revisión de la gestión de riesgos debe estar alineado con la dimensión "Control interno" del MIPG.

Producto de la evaluación independiente realizada, el Asesor de Control Interno genera un informe sobre el estado de los controles, su ejecución y efectividad en la mitigación de los riesgos identificados.

- **Ajustes a los mapas de riesgos**

Posterior a la emisión del informe emitido por el Asesor de Control Interno, los procesos con acompañamiento del Grupo Interno de Trabajo Planeación deben realizar los ajustes a sus riesgos y controles a los que haya lugar, estos cambios deben ser aprobados por el líder del proceso y la Coordinación del Grupo Interno de Trabajo Planeación con el fin de que los ajustes realizados sean incluidos en los mapas que serán objeto de revisión en el siguiente seguimiento.

11. Lineamientos para la administración del riesgo relacionado con posibles actos de corrupción

RIESGOS DE CORRUPCIÓN

Por definición, los riesgos de corrupción son la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. "*Esto implica que las 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*" (CONPES N° 167 de 2013).

A manera de ilustración a continuación se señalan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la Unidad podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos:

Direccionamiento estratégico (alta dirección)	• Concentración de autoridad o exceso de poder. Extralimitación de funciones. • Ausencia de canales de comunicación. • Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto)	• Inclusión de gastos no autorizados. • Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. • Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. • Inexistencia de archivos contables. • Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	• Estudios previos o de factibilidad deficientes. • Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). • Pliegos de condiciones hechos a la medida de una firma en particular.

	• Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). • Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. • Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. • Urgencia manifiesta inexistente. • Concentrar las labores de supervisión en poco personal. • Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	• Ausencia o debilidad de medidas y/o políticas de conflictos de interés. • Concentración de información de determinadas actividades o procesos en una persona. • Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. • Ocultar la información considerada pública para los usuarios. • Ausencia o debilidad de canales de comunicación
De Investigación y Sanción	• Inexistencia de canales de denuncia interna o externa. • Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. • Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. • Exceder las facultades legales en los fallos.
De trámites y/o servicios internos y externos	• Cobros asociados al trámite. • Influencia de tramitadores. • Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos)	• Falta de procedimientos claros para el trámite

	• Imposibilitar el otorgamiento de una licencia o permiso. • Tráfico de influencias: (amiguismo, persona influyente).

Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6

Cabe señalar que en la UPIT para la identificación de riesgos de corrupción se puede hacer uso de fuentes de datos externas como por ejemplo las de los organismos reguladores (Contraloría General de la República, Superintendencias, etc.) y del propio sector, instancias que cuentan con información global sobre situaciones irregulares que pueden llegar a ser comunes en las entidades públicas y que sirven de referente para los análisis que le son propios a cada organización.

Para el caso de fuentes internas, se pueden incluir entrevistas con el personal adecuado, la revisión de las denuncias interpuestas a través de los mecanismos implantados (canales de denuncia) y otros procedimientos analíticos. De igual forma, es pertinente incluir la evaluación de incentivos, las presiones, la potencial eliminación de controles por parte de la dirección, así como el análisis de aquellas áreas donde los controles son débiles o no existe una adecuada segregación de funciones.

Otro factor interno es la tecnología, por lo que se deben considerar los accesos a los sistemas, las amenazas internas y externas a la integridad de los datos, la seguridad de los sistemas y el posible robo de información confidencial o sensible.

11.1. Identificación del Riesgo de Corrupción

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre estos y los riesgos de gestión, en la UPIT se utiliza la matriz de definición de riesgo de corrupción, que incorpora aspectos que determinan la tipificación de este tipo de riesgos; los aspectos validadores son:

- Desviar la gestión de lo público
- Beneficio privado
- Acción u omisión
- Uso del poder

De acuerdo con la matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

Descripción del Riesgo	Acción u Omisión	Uso del Poder	Desviar la Gestión de los publico	Beneficio Privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a	**X**	**X**	**X**	**X**

nombre propio o de terceros con el fin de celebrar un contrato.				

Ejemplo tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 del DAFP

Los riesgos de corrupción se establecen sobre procesos y deben estar descritos de manera clara y precisa; su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos, por tanto, en la redacción se sugiere utilizar palabras que establezcan con claridad la tipificación de un acto de corrupción, por ejemplo, en la redacción de un riesgo de corrupción:

NO DIGA	DIGA
Pérdida de bienes	Sustracción de bienes
Pérdida de información	Ocultamiento de información
Nombramientos sin el cumplimiento de requisitos	Nombramientos irregulares
Incumplimiento de procedimientos	Omisión intencional de los requisitos o actividades de un procedimiento.

11.2. Valoración de Riesgos de Corrupción

En este paso, se debe establecer la ***probabilidad*** de ocurrencias del riesgo de corrupción, así como el nivel de consecuencia o el ***impacto*** que tendría en la Unidad si se llegara a materializar

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de **frecuencia o factibilidad**, donde frecuencia implica analizar el ***número de eventos presentados 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 de los riesgos de corrupción**

Teniendo en cuenta que para los riesgos de corrupción la probabilidad está ligada al ***número de eventos presentados en un periodo determinado,*** en la Unidad se utilizará la siguiente matriz para su determinación[6]

[6] la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 del DAFP establece los niveles: *Casi seguro, Probable, Posible, Improbable y Rara vez*, sin embargo, en la UPIT para evitar confusiones, se utilizarán los mismos niveles de la matriz de riesgo de gestión.

NIVEL	CONCEPTO	FRECUENCIA
Muy Alta	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
Alta	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
Media	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
Baja	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
Muy baja	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.

- **Criterios para calificar el impacto de los riesgos de corrupción**

Para determinar el impacto inherente de los riesgos de corrupción, se deben responder el cuestionario compuesto por 19 preguntas definidas por la Secretaría de Transparencia de la Presidencia de la República, posteriormente y de acuerdo con el número de respuestas afirmativas se determinará el nivel de impacto.

A continuación, se presenta el cuestionario que debe ser aplicado para determinar el impacto de los riesgos de corrupción

Criterios para calificar el impacto en riesgos de corrupción

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA....	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la entidad?		
4	¿Afectar el cumplimiento de la mision del sector al que pertenence la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su repotación ?		
6	¿generar pérdidad de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas genera un impacto MOEDRADO			
Responder afirmativamente de SEIS a ONCE preguntas genera un impacto MAYOR			
Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto CATASTRÓFICO			

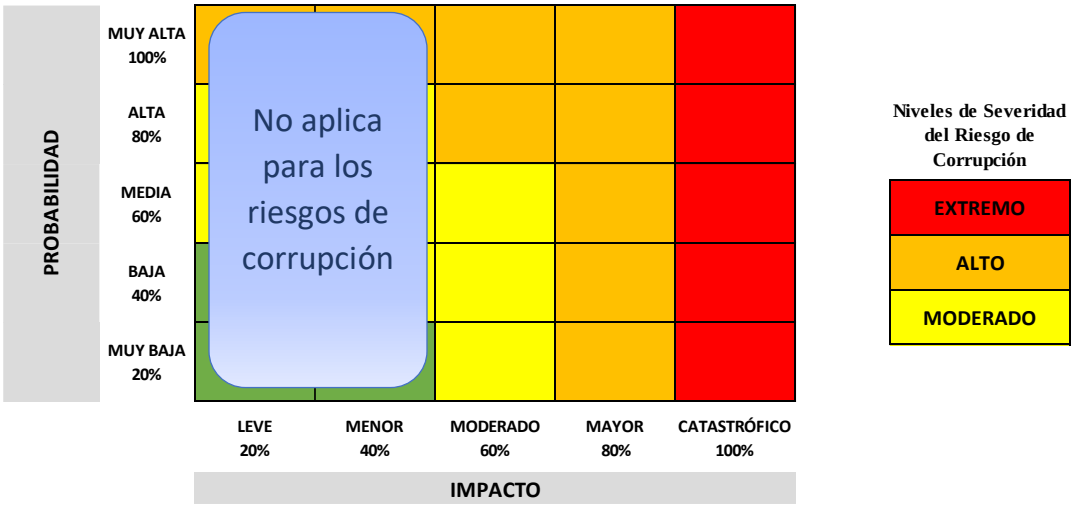
Adaptado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

Nota: Si la respuesta a la pregunta No. 16 es **es** afirmativa, el riesgo se considera catastrófico independientemente el número de preguntas contestadas afirmativamente.

Para los riesgos de corrupción, la calificación del impacto se realizará teniendo en cuenta solamente los niveles **"moderado", "mayor" y "catastrófico"**, dado que estos riesgos, de materializarse, siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto **leve ni menor**, que sí aplican para los demás riesgos.

11.3. Análisis del impacto preliminar o Inherente en riesgos de corrupción

Siguiendo la metodología y comparando el nivel de probabilidad y de impacto de los riesgos de corrupción, se ubica en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente. Para el caso de los riesgos de corrupción solo se definen 3 zonas de severidad en la matriz de calor



11.4. Valoración de los controles para Riesgos de Corrupción

En esta es etapa de la administración del riesgo, se realiza la descripción detallada y calificación de los controles asociados al riesgo de corrupción.

Para adelantar la calificación de los controles, se deben realizar los siguientes pasos:

1. Identificar y describir cada una de las características de los controles (preventivos o detectivos), que pueden disminuir la probabilidad de ocurrencia o mitigar el impacto del riesgo.

2. Evaluar los controles a partir de su operación y la información documentada sobre las características de estos.

3. Con base en los resultados consolidados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo.

11.4.1. Paso 1. Identificar y describir controles

Los controles son las acciones que los procesos han definido o implementado para minimizar la probabilidad de ocurrencia y/o el impacto del riesgo de corrupción. Los controles deben estar directamente relacionados con las causas, se sugiere que para cada causa se identifique uno o varios controles.

La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan los aspectos mínimos que se deben tener en cuenta al momento de formular adecuadamente los controles:

Nombre: Asignar un nombre al control que debe tener explicita la ejecución de una acción;

Descripción: El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo.

Propósito: El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas.

Documentación: Se debe indicar el nombre del documento del proceso en el cual se describe el control y su forma de ejecución. No es una opción válida para este campo indicar de forma genérica, que se encuentra en los documentos del proceso.

Responsable: Persona asignada para ejecutar el control; la persona asignada, debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas (Riesgos de corrupción).

Cuando un control se hace de manera manual (ejecutado por personas) es importante establecer el cargo responsable de su realización; cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es importante establecer como responsable de ejecutar el control al sistema o aplicación.

Se debe evitar asignar áreas o equipos de trabajo de manera general o nombres de personas, el control debe estar asignado a un cargo especifico.

Periodicidad: el control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Hay controles que no tienen una periodicidad específica como, por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores solo se ejecutan cuando se contratan proveedores. La periodicidad debe quedar redactada de tal forma que indique que, cada vez que se desarrolla la actividad se ejecuta el control.

Observaciones o desviaciones: El control en su diseño debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control, estableciendo el camino a seguir cuando se detectan deficiencias en el producto o servicio que se está controlando.

Evidencias de aplicación: El control debe dejar evidencia de su ejecución. Esta evidencia debe permitir validar la información por parte de un tercero

Finalmente, y una vez se hayan identificado los controles, se debe determinar a qué clase de control pertenece; los controles de los riesgos de corrupción pueden ser de dos clases, preventivos o detectivos:

Preventivos: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Estos controles intentan evitar las ocurrencias de los riesgos que puedan afectar el cumplimiento de los objetivos

Detectivos: Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones pertinentes

11.4.2. Paso 2. Evaluar los controles

Para la adecuada mitigación de los riesgos de corrupción, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Por esto, a continuación, se presenta la forma de evaluar el diseño de los controles, a partir de realizar las siguientes preguntas:

Criterio de Evaluación	Aspecto Para Evaluar en el diseño del control	Opciones de respuesta			Peso de la pregunta
Descripción	¿La fuente de la información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable		No Confiable	15
Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir	Detectar	No es control	Prevenir 15 Detectar 10
Responsable	¿Existe un responsable asignado para la ejecución del control?	Asignado		No asignado	15
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la	Adecuado		Inadecuado	15

Criterio de Evaluación	Aspecto Para Evaluar en el diseño del control	Opciones de respuesta			Peso de la pregunta
	ejecución del control?				
Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna		Inoportuna	15
Observaciones o Desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente		No se investigan y resuelven oportunamente.	15
Evidencia de aplicación del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta	No existe evidencia	Completa 10 Incompleta 5

Resultados de la evaluación del diseño del control

El resultado de la evaluación de cada criterio va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

La suma de la calificación obtenida en cada criterio determinará la calificación el control y el promedio de las calificaciones de todos los controles definidos para cada riesgo permitirá establecer la calificación del conjunto de controles

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

Si el resultado de las calificaciones del control o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados

Resultados de la evaluación de la ejecución del control

No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute y se ejecute bien. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se revalida con las actividades de evaluación realizadas por auditoría o control interno.

Rango de calificación de la Ejecución del Control	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.

Definición de la solidez individual del control

Para definir la solidez individual del control, analizaremos los resultados obtenidos en la evaluación del diseño y de la ejecución del control. 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*** individual de cada control asumirá la calificación del diseño o ejecución con menor puntaje; tal como se detalla en la siguiente tabla:

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL Fuerte: 100 Moderado: 50 Débil: 0	ESTABLECER ACCIONES DE FORTALECIMIENTO DEL CONTROL
Fuerte: Calificación entre 96 y 100	Fuerte (Siempre se ejecuta)	Fuerte + Fuerte = Fuerte	No
	Moderado (algunas veces)	Fuerte + Moderado = Moderado	Si
	Débil (No se ejecuta)	Fuerte + Débil = Débil	Si
Moderado: Calificación entre 86 y 95	Fuerte (Siempre se ejecuta)	Moderado + Fuerte = Moderado	Si
	Moderado (algunas veces)	Moderado + Moderado = Moderado	Si
	Débil (No se ejecuta)	Moderado + Débil = Débil	Si
Débil: calificación entre 0 y 85	Fuerte (Siempre se ejecuta)	Débil + Fuerte = Débil	Si
	Moderado (algunas veces)	Débil + Moderado = Débil	Si
	Débil (No se ejecuta)	Débil + Débil = Débil	Si

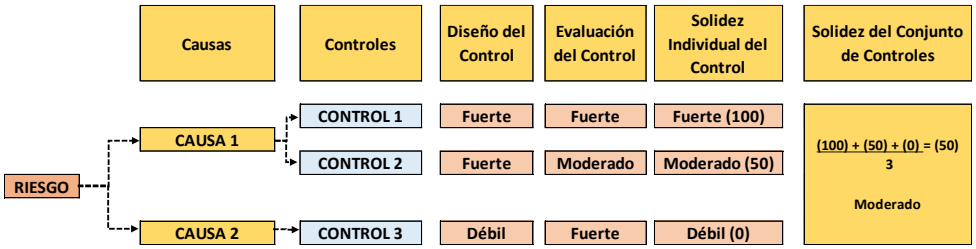
Definición de la solidez del conjunto de controles

Dado que un riesgo puede tener varias causas y a su vez, varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo, es decir la solidez que en conjunto presentan los controles de un riesgo.

La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de la solidez individual de cada control por cada riesgo.

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 esta entre 50 y 90
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Ejemplo del cálculo de la solidez del conjunto de controles:



11.4.3. Paso 3. Evaluación del Riesgo Residual

El riesgo residual hace referencia a la calificación del riesgo después de analizar y evaluar los controles definidos por el proceso.

Una vez calculado el riesgo inherente de acuerdo con lo establecido en el punto 8.2 de este documento y definido la solidez del conjunto de controles definidos para el riesgo identificado, se procede a realizar la evaluación del riesgo residual, es decir el desplazamiento que tiene un riesgo inherente en su probabilidad; es importante recalcar que, ***para los riesgos de corrupción, los controles no disminuyen el impacto, por lo consiguiente no opera desplazamiento en las columnas del eje impacto***.

El cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

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

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

11.5. Etapa Manejo de los Riesgos de Corrupción

Una vez se determine el riesgo residual, es necesario asociar la opción de manejo, que es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

El manejo de los riesgos de corrupción se realizará de acuerdo con los lineamientos establecidos en el numeral ***10.5.3 Estrategias para combatir el riesgo*** del presente manual, haciendo la salvedad de que para los riesgos de corrupción no opera la opción "Aceptar el Riesgo"

11.6. Monitoreo, seguimiento y evaluación de la gestión del riesgo de corrupción.

El monitoreo, seguimiento y evaluación de la gestión de los riesgos de corrupción, se realizará de acuerdo con los lineamientos establecidos en el numeral ***10.5.5 Monitoreo y Revisión*** del presente manual.

12. Lineamientos para la administración de Riesgos de Seguridad de la Información

La política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: *seguridad de la información, arquitectura, servicios ciudadanos digitales*.

12.1. Identificación de los activos de seguridad de la información

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: - Procesos institucionales -Aplicaciones de la organización -Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Pasos para la identificación de activos de información

De acuerdo con el "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas" los pasos para la identificación de activos son:

Adaptado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

12.2. Identificación del Riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, se toma como base de conocimiento el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla 5. Tabla de amenazas comunes
- Tabla 6. Tabla de amenazas dirigida por el hombre
- Tabla 7. Tabla de vulnerabilidades comunes

Los responsables de la identificación de los riesgos de seguridad digital pueden igualmente utilizar otras fuentes de conocimiento como:

Common Weakness Enumeration cwe.mitre.org
Common Vulnerability Exposure cve.mitre.org
Open Web Application Security Project owasp.org

Cybersecurity and Infrastructure Security Agency (CISA)
Catalogo de elementos de la guía de riesgos Magerit (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)

A continuación, se observa un ejemplo de identificación del riesgo sobre un activo como puede ser la base de datos de nómina de la entidad.

Riesgo	Activo	Descripción del Riesgo	Amenaza	Tipo	Causas / Vulnerabilidades	Consecuencias
Perdida de integridad	Base de datos de nómina	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina	Modificación no autorizada	Seguridad Digital	Políticas de Seguridad débiles Debilidades es los controles de acceso a los sistemas de información Contraseñas débiles o que no cumplen las políticas de seguridad digital Autenticación débil	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano Ej.: posible retraso en el pago de nómina

Tomado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

12.3. Valoración del Riesgo de Seguridad de la Información

Para la valoración de los riesgos de seguridad de la información se aplicará la misma metodología establecida en el numeral 10.5 del presente manual

12.4. Controles asociados a la seguridad de la información

La UPIT podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2022 y su guía de implementación de controles ISO/IEC 27002:2002, y la resolución 0500 del año 2021 del Ministerio de las Tecnologías de información y las comunicaciones.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	**Control**: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	**Control**: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	**Control**: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	**Control**: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	**Objetivo**: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	**Control**: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	**Objetivo**: proteger la información contra la perdida de datos.
Respaldo de información	**Control**: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los

	sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

12.5. Valoración de Controles de Seguridad de la Información

Para la valoración de los controles de seguridad de la información se aplicará la misma metodología establecida en el numeral 10.5.2.2 del presente manual

12.6. Estructura para la descripción del Control de Seguridad de la Información

Para la adecuada estructura de la redacción de los controles de seguridad de la información se aplicará la misma metodología establecida en el numeral 10.5.2.2 *Valoración de los Controles* del presente manual,

12.7. Tipología de controles y análisis y evaluación de los controles y atributos en seguridad de la información

Para la adecuada identificación de los controles y la evaluación de estos junto con sus atributos en seguridad de la información se aplicará la misma metodología establecida en el los numerales numeral *10.5.2.2 Valoración de Controles y 10.5.2.3. Análisis y evaluación de los controles y sus atributos* del presente manual.

12.8. Manejo del Riesgo de Seguridad de la Información.

Para el adecuado manejo del riesgo como lo recomienda el anexo 4 *"Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas"* utilizaremos el manejo de riesgo con la misma metodología establecida en el los numerales numeral 10.5.3 *Estrategias para combatir el riesgo* del presente manual.

Las demás actividades como monitoreos y seguimientos se realizarán de la misma manera que se enmarca en el presente manual para el riesgo de gestión, por otra parte, el registro y reporte de incidentes será llevado en los formatos que autorice el GIT Planeación de la UPIT para este propósito, y los establecidos por Los equipos de respuesta a incidentes de seguridad CSIRT para ser enviados a dicha entidad.

13. Lineamientos para el análisis del Riesgo Fiscal

13.1. Control fiscal interno y prevención del riesgo fiscal:

El presente aparte, tiene como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el ***daño al patrimonio público***, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado[7]

Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000. Para tener claro el ámbito normativo y jurídico, es necesario precisar que sus bases están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, los cuales fueron modificados por el Acto Legislativo 04 de 2019 que se fundamentó en la necesidad de un ejercicio preventivo del control fiscal, que detuviera el daño fiscal e identificara riesgos fiscales; de esta manera, la administración y el gestor fiscal podrían adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública.

A partir de lo anterior, el control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante, buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, con lo cual surgen conceptos clave como:

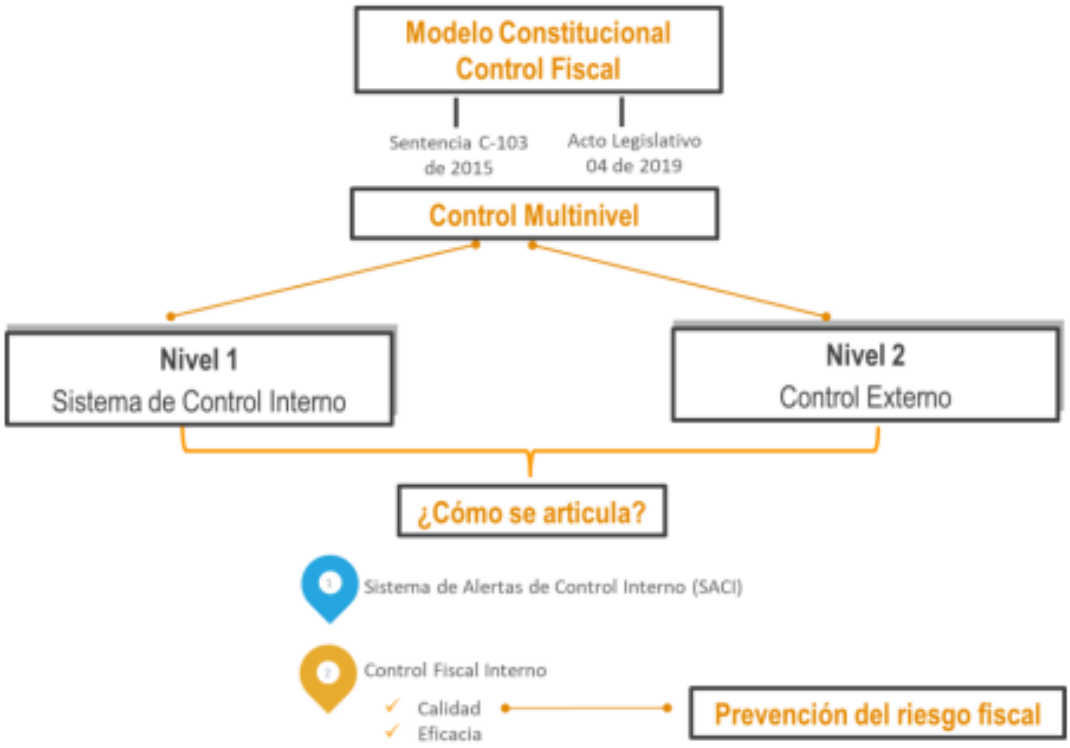
Control fiscal Multinivel: Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación del control social.

Control fiscal Interno (CFI): Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad **de todos los servidores públicos** y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

[7] Decreto 403 del 2020, art.6

El control externo adquiere un enfoque preventivo y a su vez el control interno potencia dicho enfoque, partiendo de la premisa de que el Sistema de Control Interno es fundamental para conjugar el logro de resultados, con la prevención de riesgos de gestión, corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labor es de cobro, entre otros), a través de la prevención de responsabilidades.

Articulación modelo constitucional control fiscal y sistema de control interno



Tomado de: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

A continuación, se presenta el paso a paso de la gestión del riesgo fiscal **(Identificación, análisis y valoración**), que debe vincularse al análisis general de los riesgos institucionales, a fin de contar con un esquema integral que facilite su seguimiento por parte de los líderes del proceso.

La metodología que se propone es de gran utilidad para gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez

permite, mitigar la posibilidad de configuración de responsabilidades fiscales para los diferentes gestores públicos.

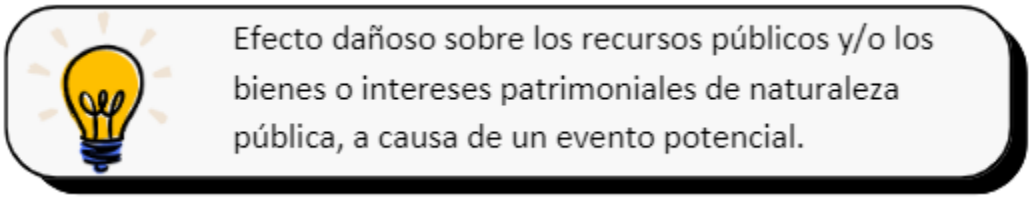
Como parte integral de la metodología propuesta el DAFP pone a disposición, como insumo de referencia, el documento borrador *Anexo_1_Catálogo_Listado.pdf*

Éste Catalogo ha sido construido como resultado del análisis de precedentes (aproximadamente 130 fallos con responsabilidad fiscal de contralorías territoriales y de la Contraloría General de la República) y debe ser utilizado como marco de referencia para la identificación y valoración de riesgos fiscales, siempre atendiendo las particularidades, naturaleza, complejidad, recursos, usuarios o grupos de valor, portafolio de productos y servicios, sector en el cual se desenvuelva (contexto), así como otras condiciones específicas de cada entidad.

En consecuencia, en Unidad se debe analizar si existen, de acuerdo con su contexto y particularidades puntos de riesgos y circunstancias inmediatas diferentes a los identificados en el mencionado catálogo y tenerlas en cuenta al momento de identificar los riesgos fiscales.

13.2. Definición y elementos del Riesgo Fiscal:

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene el presente documento, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:



Los elementos que componen la definición de riesgo fiscal son:

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

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal; se relaciona con una potencial acción u omisión [8]que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz que ocasiona el efecto.

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal= Evento Potencial (Potencial Conducta) + Efecto Dañoso (Potencial Daño)

13.3. Metodología para el levantamiento del mapa de riesgos fiscales

De la misma manera que se ha realizado para los demás tipos de riesgos, la administración de los riesgos fiscales en el presente manual se adelantará siguiendo los lineamientos establecidos para ***identificar, clasificar, valorar y controlar*** los riesgos fiscales definidos, que es fundamental para el resultado de la gestión de cada entidad y para la seguridad y prevención de responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros).

13.3.1. Paso 1 Identificación de Riesgos Fiscales

Para la identificación del riesgo fiscal es necesario establecer los **puntos de riesgo fiscal** y las **circunstancias o causas Inmediatas**.

Los **puntos de riesgos** son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de *administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición* de los bienes o recursos públicos, así como a la *recaudación, manejo e inversión de sus rentas*[9] . En conclusión, los puntos de riesgo fiscal son **todas las actividades que representen**

[8] El DAFP en el borrador del documento **Identificación y valoración de riesgos fiscales y diseño de controles para su prevención y mitigación** hace referencia a *potencial conducta dolosa o gravemente culposa*

9 Artículo 3 Ley 610 de 2000.

gestión fiscal, en las **cuales se han generado de manera persistente se presentan advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal**

Las **circunstancias o causas inmediatas** hacen referencia a aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, pueden existir múltiples circunstancias inmediatas.

Para identificar los **puntos de riesgo** y las **circunstancias inmediatas**, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que 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 circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal). Para este taller, puede usar las siguientes preguntas orientadoras:

Sirve para Identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver la definición de gestión fiscal)
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar la metodología propuesta el DAFP pone a disposición, como insumo de referencia, el documento borrador *Anexo_1_Catálogo_Listado.pdf*
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.

Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas", son aplicables a la entidad?

Tomado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

13.3.2. Identificación de Áreas de Impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio de la Entidad, a la cual se vería expuesta la UPIT en caso de materializarse el riesgo. Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

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

(i) Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.
(ii) Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el numeral 3. Glosario del presente documento).

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: Bienes Públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública (consultar definiciones en el numeral 3. Glosario de este documento.

13.3.3. Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse 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) 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 de la Unidad.

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño -efecto- (Contraloría General de la República, 2021)[10]

Ejemplo:
La entidad se atrasó en el pago del canon de arrendamiento de sus oficinas por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

¿Cuál es el daño?
El daño fiscal corresponde al monto pagado por concepto de intereses moratorios.

¿Cuál es el hecho generador?
La omisión de pagó oportuno del canon de arrendamiento.

Conclusión
El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

[10] Concepto CGR-OJ-115 -2021 de la Contraloría General de la República, pág. 13

13.3.4. Descripción del Riesgo Fiscal

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

Para redactar un riesgo fiscal se debe tener en cuenta:

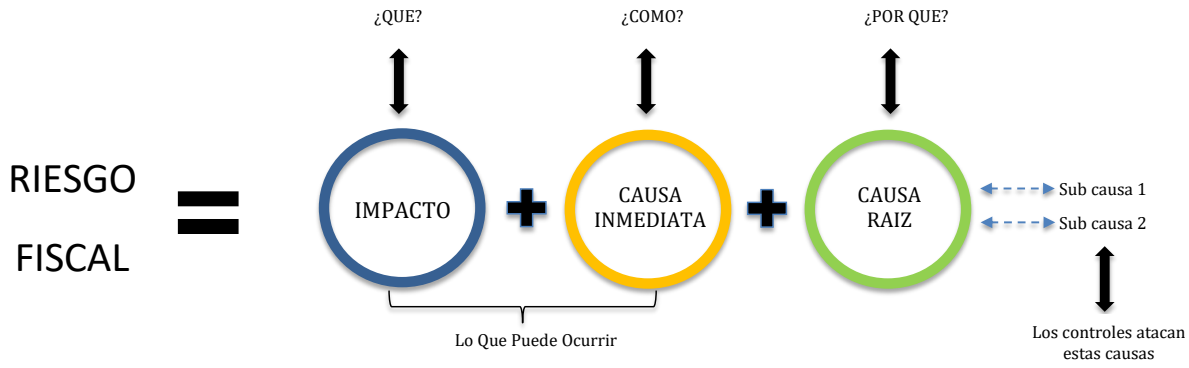
✓ **Iniciar con la oración**: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.

✓ **Impacto:** Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

✓ **Circunstancia inmediata**: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

✓ **Causa Raíz**: Corresponde al por qué; 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[11]

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



[11] El control fiscal y la responsabilidad fiscal en Colombia. Luz Jimena Duque Botero y Fredy Céspedes Villa. Ibáñez 2018

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 06

Ejemplo:
Proceso: Gestión Administrativa

Objetivo: Gestionar y administrar los servicios, bienes muebles e inmuebles y transporte de la UPIT garantizando su mantenimiento y custodia contribuyendo en la eficiencia y sostenibilidad de los recursos.

Alcance: Inicia con la identificación de necesidades de servicios, bienes muebles e inmuebles y transporte, siguiendo con la verificación de disponibilidad y asignación a los servidores públicos y posterior manifestación a satisfacción, continúa con el control, custodia y proceso de baja de los bienes en desuso por obsolescencia.

¿QUE?	¿COMO?	¿POR QUÉ?
Posibilidad de efectos dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Como complemento a continuación se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso, es decir efecto dañoso sobre bienes públicos, recursos públicos o sobre intereses patrimoniales de naturaleza pública

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	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

	la licencia ambiental de los proyectos de infraestructura.	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

13.3.5. Paso 2 Valoración del Riesgo Fiscal

Evaluación de riesgos

La valoración del riesgo fiscal hace referencia a las actividades que se deben seguir al interior de la UPIT para determinar la probabilidad y el impacto inherente, para lo cual seguiremos los lineamientos establecidos para la valoración de los riesgos de gestión que se encuentran en el numeral 10.5.1 de este documento.

Probabilidad

La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal. Teniendo esto de presente, para definir el nivel de probabilidad, se debe tener en cuenta la siguiente tabla definida en el numeral 10.5.1.1 de la presente guía:

Impacto

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública. Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales, sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal, se aplicará la siguiente tabla definida en el numeral 10.5.1.2 del presente manual:

Determinación del nivel de riesgo inherente

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad en la matriz de calor, para lo cual se aplica la matriz definida en el numeral 10.5.2.1 del presente manual en donde se definen 4 zonas de severidad; Extremo, Alto, Moderado y Bajo

Ejemplo (continuación):

Proceso: Gestión Administrativa

Objetivo: Gestionar y administrar los servicios, bienes muebles e inmuebles y transporte de la UPIT garantizando su mantenimiento y custodia contribuyendo en la eficiencia y sostenibilidad de los recursos.

Alcance: Inicia con la identificación de necesidades de servicios, bienes muebles e inmuebles y transporte, siguiendo con la verificación de disponibilidad y asignación a los servidores públicos y posterior manifestación a satisfacción, continúa con el control, custodia y proceso de baja de los bienes en desuso por obsolescencia.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos **(área de impacto)**, por pérdida, extravío o hurto de bienes muebles de la entidad **(circunstancia inmediata)**, a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar **(causa raíz).**

Probabilidad: Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta que los bienes muebles en cada entidad varían en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.

Aplicando las tablas de probabilidad e impacto tenemos:

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

La actividad se realiza 365 veces al año, la probabilidad de ocurrencia del riesgo es **MEDIA**.

Ahora, para determinar el **impacto** es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública. En este ejemplo el efecto dañoso sería del valor contable del inventario de **bienes muebles** que para el ejemplo se determina que es de $500 millones de pesos, lo cual corresponde a 384 SMLMV[12]. De acuerdo con la tabla para la definición del nivel de impacto de la UPIT, este riesgo tiene un nivel de impacto **MAYOR**

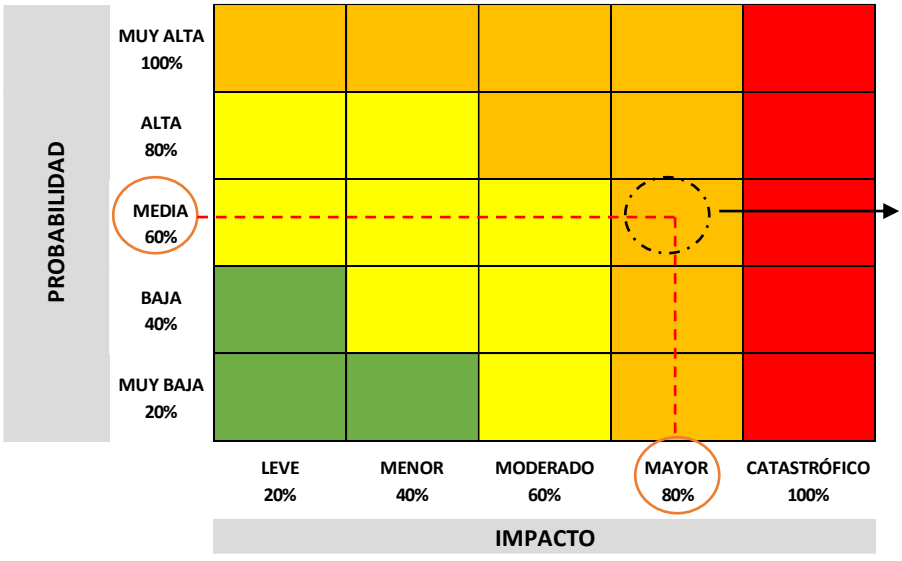
[12] Se toma como base el Salario Mínimo de 2024

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

La afectación económica se calculó en 384 SMLV, el impacto del riesgo es **MAYOR**

Probabilidad inherente= MEDIA 60%, **Impacto inherente**: MAYOR 80%

Zona de severidad o nivel de riesgo: De acuerdo con la tabla para la definición de zona severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un nivel de riesgo ALTO.



Cruzando los datos de probabilidad e impacto definidos, el riesgo inherente se ubica en zona de riesgo **ALTA**

13.3.6. Paso 3 Valoración de Controles para Riesgo Fiscal

Como todos los riesgos que se tratan en este manual, los riesgos fiscales cuentan con acciones que buscan evitar que se materialicen dichas situaciones o mitigar el impacto en caso de que suceda. Estas acciones son conocidas como Controles o Acciones de Control.

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

Tipología y valoración de los controles

La tipología de los controles de los riesgos fiscales, así como los lineamientos para la correcta descripción de las acciones de control, serán los mismos que se determinaron en el numeral 10.5.2.2 del presente documento

Análisis y evaluación de los controles

Para el análisis y evaluación de los controles se aplicarán los mismos lineamientos establecidos en el numeral **10.5.2.3 Análisis y evaluación de los controles** del presente manual

Nivel de Riesgo o Riesgo Residual:

Corresponde al resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control tal como se establece en el numeral **10.5.2.4 Nivel de Riesgo o Riesgo Residual**

Estrategias para combatir el riesgo fiscal

De acuerdo con la zona en donde quede ubicado el riesgo residual, se debe proceder con la determinación de las opciones de manejo del riesgo fiscal, para lo cual se deben seguir los lineamientos establecidos en el numeral **10.5.3 Estrategias para combatir el riesgo** del presente documento.

14. ¿Qué cambios ha tenido el documento?

Versión Generada	Fecha	Descripción del Cambio o Modificación
01	2/08/2024	Versión inicial del documento aprobado por comité en sesión ordinaria.

Elaboró	Revisó	Aprobó
Willington Granados Herrera Profesional Especializado GIT Planeación **Jhon Alexander Gómez Arévalo** Contratista GIT Planeación	**Johana Paola Lamilla Sánchez** Coordinadora Grupo Interno de Trabajo de Planeación	Comité Institucional de Coordinación del Sistema de Control Interno de la Unidad de Planeación de Infraestructura de Transporte