POLÍTICA INSTITUCIONAL PARA LA ADMINISTRACIÓN DEL RIESGO

Historia de revisiones.

Versión	Fecha	Por	Resumen de Cambios
01	03/05/2021	Milena Farina Rodríguez Flórez Profesional de planeación	Versión inicial del documento
02	03/08/2023	Román Fernando Gómez Marín Líder de Planeación	-Se ajusta la redacción en diferentes secciones de la política, para precisar los lineamientos sobre la gestión del riesgo. -Se actualizan las referencias externas a las versiones más recientes de los documentos de apoyo del MIPG emitidos por el DAFP. -Se ajusta el alcance y se incluyen los términos y lineamientos relativos a la gestión del riesgo fiscal, para adecuarse a lo establecido en la versión 6 de la "*Guía para la administración del riesgo y el diseño de controles en las entidades públicas*" del DAFP.

Aprobación.

Elaborado	Revisado	Aprobado
Nombre: Román Fernando Gómez Marín	**Nombre:** Román Fernando Gómez Marín	**Nombre:** Comité Institucional de Coordinación de Control Interno (CICCI)
Cargo: Líder de planeación	**Cargo:** Líder de planeación	**Cargo:** N.A.
Fecha: 03/08/2023	**Fecha:** 09/08/2023	**Fecha:** 05/09/2023

Tabla de contenido

1. Objetivo.

Establecer los criterios orientadores que definan el marco general de referencia para la administración de los riesgos en todos los procesos de Teleantioquia, buscando minimizar su posibilidad de ocurrencia y asegurar que su eventual materialización no afecte el logro del propósito misional ni el cumplimiento de los objetivos institucionales.

2. Resultados esperados.

- ✓ Metodología para la administración del riesgo en Teleantioquia actualizada y definida según los lineamientos del Departamento administrativo de la función pública (DAFP).
- ✓ Lineamientos adoptados para la identificación, valoración, tratamiento y seguimiento unificado de los riesgos en todos los procesos del canal, según lo establecido en la norma técnica ISO 31000.
- ✓ Mitigación o eliminación de pérdidas económicas y de afectaciones al logro de los objetivos institucionales, ocasionadas por la materialización de riesgos.
- ✓ Preservación de la buena imagen y las buenas relaciones de la entidad con sus grupos de interés.
- ✓ Protección de los bienes y recursos de Teleantioquia, resguardándolos contra la materialización de riesgos.
- ✓ Integración de la gestión de riesgos en todos los procesos del canal, para fortalecer y mejorar la toma de decisiones.
- ✓ Mejora continua en los procesos y procedimientos de la institución, a partir del monitoreo y seguimiento periódico de los riesgos, asegurando la eficacia y eficiencia de los controles establecidos para su tratamiento.
- ✓ Fomento de la cultura de prevención del riesgo en todos los niveles de la entidad.

3. Alcance.

La Política de Administración de riesgos es aplicable a todos los procesos, programas, proyectos y planes institucionales, así como a todos los servidores públicos, empleados temporales y contratistas de prestación de servicios que realizan actividades o tareas para Teleantioquia.

Incluye lineamientos para el tratamiento, manejo y seguimiento a los riesgos de gestión, corrupción, fiscales y de seguridad de la información, los cuales se gestionarán únicamente para los activos de seguridad de la información con nivel de criticidad ***Alto***.

4. Definiciones[1].

- **Aceptación de riesgo:** decisión informada de aceptar las consecuencias y probabilidades de un riesgo en particular.

[1] Construcción propia a partir de los conceptos enunciados en la "***Guía para la administración del riesgo y el diseño de controles en las entidades públicas***", versión 6 (2022), del Departamento Administrativo de la Función Pública (DAFP); la norma ISO 31000:2018 (NTC/ISO 31000:2018) "***Gestión de Riesgos - Principios y Directrices***", la guía ISO 73:2009 "***Gestión de Riesgos -***

- **Activo:** en el contexto de seguridad de la información, 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.
- **Administración de riesgos:** cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.
- **Amenaza:** peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales.
- **Análisis de riesgo:** uso sistemático de la información disponible para determinar cuán frecuentemente pueden ocurrir eventos especificados, y la magnitud de sus consecuencias.
- **Apetito de riesgo:** es el nivel de riesgo que la entidad está dispuesta a aceptar, en la búsqueda de sus objetivos, dentro del 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.
- **Bienes de uso público:** aquellos bienes públicos cuyo uso pertenece a todos los habitantes del territorio nacional (las calles, plazas, puentes, vías, parques, etc.).
- **Bienes fiscales:** aquellos bienes públicos que están destinados al cumplimiento de las funciones o servicios públicos a cargo del estado, es decir, afectos al desarrollo de su misión y utilizados para sus actividades (terrenos, edificios, oficinas, colegios, hospitales, fincas, granjas, equipos, enseres, mobiliario, etc.).
- **Bienes públicos:** todos aquellos muebles e inmuebles de propiedad pública (comprende bienes del estado y aquellos productos del ejercicio de una función pública a cargo de particulares); se clasifican en bienes de uso público y bienes fiscales.
- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar en la búsqueda de sus objetivos institucionales, y a partir del cual se considera por la alta dirección y el órgano de gobierno que no sería posible el logro de los mismos.
- **Causas:** factores internos y externos que son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores se entienden como todos los sujetos

Vocabulario", la norma técnica ISO 9001:2015 (NTC/ISO 9001:2015) "***Sistemas de Gestión de la Calidad***" y el "***Marco integrado para la administración de riesgos empresariales***", versión 2017, del Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO).

u objetos que, solos o en combinación con otros, tienen la capacidad de originar o materializar un riesgo.

- **Causa Inmediata:** circunstancia bajo la cual se presenta el riesgo, pero no constituye la causa principal o base para que se presente el riesgo.
- **Causa raíz:** causa principal o básica, corresponde a la razón por la cual se puede presentar el riesgo.
- **Compartir o transferir el riesgo:** reducir su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros, o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones. La revelación no autorizada de la información calificada de acuerdo con un nivel de confidencialidad alto implica un grave impacto para una entidad en términos económicos y de su imagen ante sus grupos de interés.
- **Conflicto de intereses:** surge cuando un servidor público tiene un interés privado que podría influir, o en efecto influye, en el desempeño imparcial y objetivo de sus funciones oficiales, porque le resulta particularmente conveniente a él, su familia, o sus socios cercanos.
- **Consecuencia:** efecto o situación resultante de la materialización del riesgo que afecta el cumplimiento de los objetivos.
- **Control:** medida que mantiene o modifica un riesgo. Los controles incluyen, pero no se limitan a, cualquier proceso, política, dispositivo, práctica u otras condiciones o acciones que mantengan o modifiquen un riesgo.
- **Control de riesgos:** la parte de administración de riesgos que involucra la implementación de políticas, estándares, procedimientos para eliminar o minimizar los riesgos adversos.
- **Controles correctivos:** permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia.
- **Controles preventivos:** actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
- **Desastre:** resultado que se desencadena de la manifestación de uno o varios eventos naturales o antropogénicos no intencionales que al encontrar condiciones propicias

de vulnerabilidad en las personas, los bienes, la infraestructura, los medios de subsistencia, la prestación de servicios o los recursos ambientales, causa daños o pérdidas humanas, materiales, económicas o ambientales, generando una alteración intensa, grave y extendida en las condiciones normales de funcionamiento de la entidad, que exige ejecutar acciones de respuesta a la emergencia, rehabilitación y reconstrucción.

- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Evaluación del riesgo:** proceso utilizado para determinar las prioridades de la administración del riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
- **Factores de riesgo:** son las fuentes generadoras de riesgos.
- **Fuente de riesgo:** elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar la organización con relación al riesgo.
- **Gestor fiscal:** servidores públicos y 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.
- **Gestor público:** es toda persona que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sea o no gestor fiscal.
- **Identificación del riesgo:** elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.
- **Impacto(s):** la(s) consecuencia(s) que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** propiedad de exactitud y completitud.
- **Intereses patrimoniales de naturaleza pública:** son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica (la rentabilidad proyectada de cualquier inversión pública, la cobertura de garantías y pólizas, la participación accionaria

pública en una empresa y los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir, antes de que se causen o generen efectivamente, etc.).

- **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 sus objetivos. En general la fórmula del nivel de riesgo es probabilidad x 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.
- **Plan anticorrupción y de atención al ciudadano (PAAC):** plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Política:** intenciones y dirección de una organización, como la expresa formalmente su alta dirección.
- **Política de administración del riesgo:** declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos
- **Probabilidad:** se entiende como la posibilidad de ocurrencia o materialización 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.
- **Puntos de riesgo:** actividades dentro del flujo de un proceso donde existe evidencia, o se tiene indicios, de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.
- **Recurso público:** para efectos de la gestión de riesgos fiscales, entiéndase como recurso público los dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Reducir el riesgo:** tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección) de materialización de un riesgo. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.

- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia el beneficio privado.
- **Riesgo de seguridad de la información:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).
- **Riesgo fiscal:** probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Riesgo inherente:** nivel de riesgo propio de una actividad. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo residual:** nivel de riesgo que permanece luego de aplicar los controles o medidas de tratamiento al riesgo inherente.
- **Tolerancia del riesgo:** es el valor admisible de desviación del nivel de riesgo en los resultados o actuaciones de la entidad con respecto al valor del Apetito de riesgo determinado.
- **Vulnerabilidad:** representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. Contexto.

Durante la vigencia 2020 Teleantioquia actualizó su plataforma estratégica en un trabajo colectivo que se materializó en el plan estratégico 2020 – 2023 "*Teleantioquia emociona*". Simultáneamente, la Oficina de planeación inició la revisión y actualización del modelo de operación por procesos y el sistema integrado de gestión del canal, para asegurar la capacidad institucional de lograr los objetivos estratégicos propuestos y contribuir a la implementación del modelo integrado de planeación y gestión (MIPG).

En 2021 Teleantioquia actualizó su política en consonancia con los objetivos estratégicos, programas y proyectos definidos en el plan estratégico institucional, el modelo de operación actualizado y con los lineamientos contenidos en la versión 5 de la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*" del DAFP, en consideración a que el MIPG establece que la estructuración de la política de administración de riesgos es una tarea que debe realizarse en conjunto con el ejercicio de direccionamiento estratégico institucional.

Teniendo en cuenta que el Departamento Administrativo de la Función Pública (DAFP) realizó el lanzamiento de la versión 6 de la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*", y que además se cumplen dos años desde la última revisión, se hace entonces necesario renovar la política actual de tal manera que se incorporen los nuevos lineamientos contenidos en la guía actualizada del DAFP y se revisen y actualicen (en caso de ser necesario) los aspectos fundamentales de la misma para asegurar su efectividad.

6. Declaración general de la política.

En Teleantioquia estamos comprometidos con la identificación, evaluación y gestión integral de los riesgos que puedan comprometer el cumplimiento de nuestros objetivos institucionales, con un enfoque preventivo que nos permita evitar, reducir o eliminar efectos indeseados como la pérdida o deterioro excepcional de los bienes y recursos públicos bajo nuestra custodia, la afectación de nuestra imagen corporativa o el deterioro de las relaciones con nuestros grupos de interés.

Nuestra gestión del riesgo se enmarca en el Modelo integrado de planeación y gestión (MIPG), tiene como referencias las directrices de sus políticas de gestión y desempeño y el esquema de líneas de defensa como elemento fundamental de la 7° dimensión (control interno) y toma como bases el direccionamiento estratégico y el modelo de operación por procesos del canal.

Para fortalecer este compromiso, la alta dirección del canal se enfocará en:

- Cumplir la normatividad vigente en Colombia, aplicable en materia de riesgos y transparencia.
- Asegurar que los recursos necesarios para gestionar los riesgos sean asignados oportunamente.
- Integrar la gestión de riesgos a todos los procesos, planes y proyectos del canal, para mejorar la toma de decisiones.
- Articular la administración de los riesgos, para que sean gestionados de manera unificada durante la identificación, valoración y tratamiento de los mismos.
- Definir las responsabilidades diferenciadas frente a la gestión del riesgo, basadas en el modelo de líneas de defensa establecido en la 7° dimensión del MIPG.
- Definir el tratamiento a los niveles de riesgo identificados en el marco de la administración del riesgo.
- Actualizar y mejorar continuamente la política para la administración del riesgo para que se adecúe a los cambios en el contexto organizacional.
- Actualizar sistemáticamente el mapa de riesgos.
- Monitorear y controlar sistemáticamente los riesgos identificados, mediante la ejecución, evaluación y ajuste de los planes de acción creados para prevenirlos y mitigarlos.

- Divulgar la política para la administración del riesgo y los mapas de riesgo y planes de acción para prevenir su materialización, de tal manera que se fortalezca la cultura de control en la organización.

7. Roles y responsabilidades frente a la gestión del riesgo[2].

Línea de defensa	Responsable	Responsabilidades
Estratégica	**Alta dirección**[3]: • Gerente • Secretario general • Directores • Líderes de área • Jefes • Coordinadores que dependen del Gerente	1. Definir e impartir los lineamientos generales para la administración del riesgo en la entidad. 2. Definir y realizar seguimiento a los niveles de aceptación de los riesgos, así como al apetito, tolerancia y capacidad del riesgo del canal. 3. Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. 4. Realizar seguimiento y supervisión periódica a la gestión de los riesgos institucionales.
	Comité institucional de coordinación de control interno (CICCI)	1. Revisar, aprobar y evaluar la política de administración de riesgos. 2. Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones para el fortalecimiento de la gestión del riesgo. 3. Analizar eventos (materialización de riesgos) y riesgos críticos. 4. Realimentar al Comité Institucional de Gestión y Desempeño los ajustes que se deben realizar frente a la gestión del riesgo. 5. Asegurar la difusión, en todos los niveles de la entidad, de la presente política institucional, de tal forma que cada una de las tres líneas de defensa conozcan claramente los niveles de responsabilidad y autoridad que posee frente a la gestión del riesgo.
	Comité institucional de gestión y desempeño (CIGD)	1. Revisar el contexto estratégico, plataforma estratégica, el modelo de operación por procesos y la planeación institucional, con el fin de analizar los posibles eventos de riesgos que se puedan materializar en el ejercicio de la labor misional. 2. Analizar la gestión del riesgo y aplicar mejoras para la misma. 3. Analizar, evaluar y aprobar el mapa de riesgos institucional, y las actualizaciones del mismo.
Primera línea	• Líderes de proceso • Líderes de subproceso • Directores de proyecto • Supervisores de contratos En conjunto con sus equipos de trabajo	1. Identificar y valorar los riesgos y controles de los procesos, subprocesos, proyectos y contratos bajo su responsabilidad, con la participación de su equipo de trabajo. 2. Implementar y monitorear los controles identificados no existentes previamente en los procesos, subprocesos, proyectos y contratos bajo su responsabilidad. 3. Realizar seguimiento y análisis a los controles de los riesgos según la periodicidad establecida. 4. Definir las mejoras a la gestión del riesgo del proceso, subproceso, proyecto o contrato bajo su responsabilidad. 5. Supervisar la ejecución de los controles y detectar las deficiencias de estos, determinando las acciones de mejora requeridas. 6. Autoevaluar la administración del riesgo: hacer seguimiento a la ejecución de controles y determinación de materialización de riesgos de gestión y corrupción. 7. Informar a la Oficina de Planeación (segunda línea) sobre los riesgos materializados, cambios en el entorno y amenazas que se identifiquen en el cumplimiento de los objetivos institucionales.

[2] Construcción propia a partir de los lineamientos enunciados en la "***Guía para la administración del riesgo y el diseño de controles en las entidades públicas***", versión 6 (2022), el "***Manual operativo del modelo integrado de planeación y gestión***", versión 4 (2021), la "***Guía para la gestión del riesgo de corrupción***" (2015) y la "***Política de administración de riesgos***", del Departamento Administrativo de la Función Pública (DAFP).

[3] Los roles que componen la alta dirección se establecieron a partir de los conceptos contenidos en el "***Manual operativo del modelo integrado de planeación y gestión***", versión 5 (2023) del DAFP, sección 7.1. "*Alcance de esta dimensión*" (de control interno), pp. 119.

Línea de defensa	Responsable	Responsabilidades
		8. Reportar a la Oficina de Control Interno (tercera línea) los avances y evidencias de la gestión de los riesgos a cargo del proceso, subproceso, proyecto o contrato.
Segunda línea	Oficina de planeación	1. Identificar los cambios en el entorno y nuevas amenazas que se puedan presentar en el cumplimiento de los objetivos institucionales. 2. Definir la metodología para la identificación, análisis, valoración y evaluación del riesgo, acorde a la normatividad y lineamientos para cada tipo de riesgo, con excepción de los riesgos que por naturaleza requieran una metodología particular (Riesgos ambientales, de seguridad de la información y de seguridad y salud en el trabajo). 3. Capacitar, acompañar metodológicamente y generar recomendaciones para la identificación, análisis, valoración y evaluación del riesgo. 4. Asegurar que los controles y procesos de gestión de riesgos de la primera línea sean apropiados y funcionen correctamente. 5. Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política para la administración de riesgos, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. 6. Consolidar el Mapa de riesgos institucional, presentarlo para su análisis, evaluación y aprobación ante el Comité Institucional de Gestión y Desempeño y publicarlo conforme a los lineamientos normativos. 7. Evaluar que la gestión de riesgos sea consistente con la política de administración de riesgos de la entidad y que éstos sean monitoreados por la primera línea de defensa. 8. Identificar los cambios en el apetito del riesgo, en especial los riesgos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno. 9. Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio. 10. Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad.
	• Secretario general • Directores • Líderes de área • Jefes • Coordinadores	1. Supervisar que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos, en cumplimiento de los lineamientos para la gestión de riesgos. 2. Asegurar que los controles y procesos de gestión de riesgos de la primera línea sean apropiados y funcionen correctamente. 3. Realizar el seguimiento al mapa de riesgos de su área. 4. Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. 5. Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad. 6. El Secretario general tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. 7. Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo.
Tercera línea	Oficina de control interno	1. Proporcionar el aseguramiento objetivo sobre la eficacia de la gestión del riesgo y el control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos, subprocesos, proyectos y contratos. 2. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. 3. Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. 4. Asesorar de manera coordinada con la Oficina Asesora de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y el diseño de los controles de los riesgos. 5. Presentar al Comité Institucional de Coordinación de Control Interno el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria. 6. Evaluar la eficacia, eficiencia y efectividad de los controles en los mapas de riesgos, y sus debilidades. 7. Recomendar mejoras a la política de administración del riesgo, y a la metodología para la identificación de los riesgos y sus controles.

Línea de defensa	Responsable	Responsabilidades
		8. Formar a la alta dirección, y a todos los niveles de la entidad, sobre las responsabilidades en materia de riesgos.

8. Metodología.

La metodología utilizada por Teleantioquia para la gestión del riesgo es una adaptación a las características propias del canal de la metodología establecida en la "*Guía para la administración del riesgo y el diseño de controles en las entidades públicas*", emitida por la dirección de gestión y desempeño del DAFP, en su versión número 6 de noviembre de 2022, y la norma técnica ISO 31000:2018 (NTC/ISO 31000:2018) "*Gestión de Riesgos - Principios y Directrices*"; incorpora también lineamientos de la "Guía para la gestión del riesgo de corrupción" del DAFP, publicada en 2015 y del documento "*Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas*" (2018), del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). La metodología es descrita detalladamente en el procedimiento documentado "***PR-101004 Gestión de riesgos***".

La gestión del riesgo toma como insumos esenciales el direccionamiento estratégico, el modelo de operación por procesos de la entidad y el análisis de su contexto y entorno, para luego identificar los factores y puntos de riesgo y clasificar los riesgos identificados (al conjunto de estas actividades se le denomina "*Identificación del riesgo*").
A continuación se analizan los riesgos detectados, se evalúa su probabilidad de ocurrencia y sus posibles consecuencias o impactos para estimar su severidad o zona de riesgo inicial (riesgo inherente) y se confrontan los resultados de la evaluación inicial frente a los controles establecidos para determinar su severidad o zona de riesgo final (riesgo residual; al conjunto de estas últimas actividades se le denomina "*Valoración del riesgo*").
Finalmente, se establecen las estrategias para combatir el riesgo ("*Tratamiento del riesgo*") y los planes de acción y periodos de seguimiento y revisión que aseguren la eliminación del riesgo o la disminución de su nivel a valores aceptables.

9. Lineamientos para el análisis de los riesgos.

El análisis es el proceso mediante el cual se busca, para un riesgo identificado, establecer su *probabilidad de ocurrencia* y su *nivel de consecuencia o impacto*, con el fin de determinar su *nivel de severidad o zona de riesgo inicial* (riesgo inherente).

9.1. Criterios para establecer la probabilidad de ocurrencia.

La probabilidad se entiende como la posibilidad de materialización del riesgo; está asociada a la exposición al riesgo en el proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo durante el transcurso de un (1) año.

En la siguiente tabla se definen los criterios para establecer la probabilidad de ocurrencia (y su valoración) para un riesgo:

Probabilidad	Porcentaje	Frecuencia de la actividad
Muy baja	20%	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.
Baja	40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.
Media	60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año.
Alta	80%	La actividad que conlleva el riesgo se ejecuta mínimo 501 y máximo 5,000 veces por año.
Muy alta	100%	La actividad que conlleva el riesgo se ejecuta más de 5,000 veces por año.

Nota: En materia de tecnología se considera que una (1) hora de funcionamiento equivale a una (1) vez.

9.2. Criterios para determinar el nivel de impacto.

Para la determinación del impacto se definieron como variables a considerar, *en los riesgos de gestión y de seguridad de la información*, las afectaciones económicas, de reputación, legales y operativas. Cuando se presenten múltiples impactos para un riesgo identificado, con diferentes niveles, se le debe asignar el nivel más alto.

Para la determinación del impacto potencial frente a posibles materializaciones de *riesgos fiscales*, debe tenerse en cuenta que estos, por su naturaleza y alcance, *producirán únicamente afectaciones de tipo económico*, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública[4].

En la determinación del impacto frente a posibles materializaciones de *riesgos de corrupción* se obtendrán únicamente niveles moderado, mayor, y catastrófico, *dado que los riesgos de corrupción siempre serán significativos*[5]; para calcular el valor correspondiente se deberán responder las preguntas definidas por el DAFP, y asignar la valoración establecida conforme a las respuestas[6], para cada riesgo de corrupción identificado.
Las preguntas y su correspondiente valoración fueron consolidadas en el formato "***FO-101012 Determinación impacto riesgo de corrupción***", para facilitar la

[4] Departamento Administrativo de la Función Pública (DAFP), "***Guía para la administración del riesgo y el diseño de controles en las entidades públicas***", versión 6 (2022), sección 4.3. "*Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales*", pp. 75
[5] Departamento Administrativo de la Función Pública (DAFP), "***Guía para la administración del riesgo y el diseño de controles en las entidades públicas***", versión 6 (2022), sección 5. "*Lineamientos sobre los riesgos relacionados con posibles actos de corrupción*", pp. 89
[6] Departamento Administrativo de la Función Pública (DAFP), "***Guía para la administración del riesgo y el diseño de controles en las entidades públicas***", versión 6 (2022), sección 5. "*Lineamientos sobre los riesgos relacionados con posibles actos de corrupción*" pp. 88

determinación del impacto respecto a este tipo de riesgo. Por lo anterior, durante el análisis *debe diligenciarse uno de estos formatos para cada uno de los riesgos de corrupción identificados*.

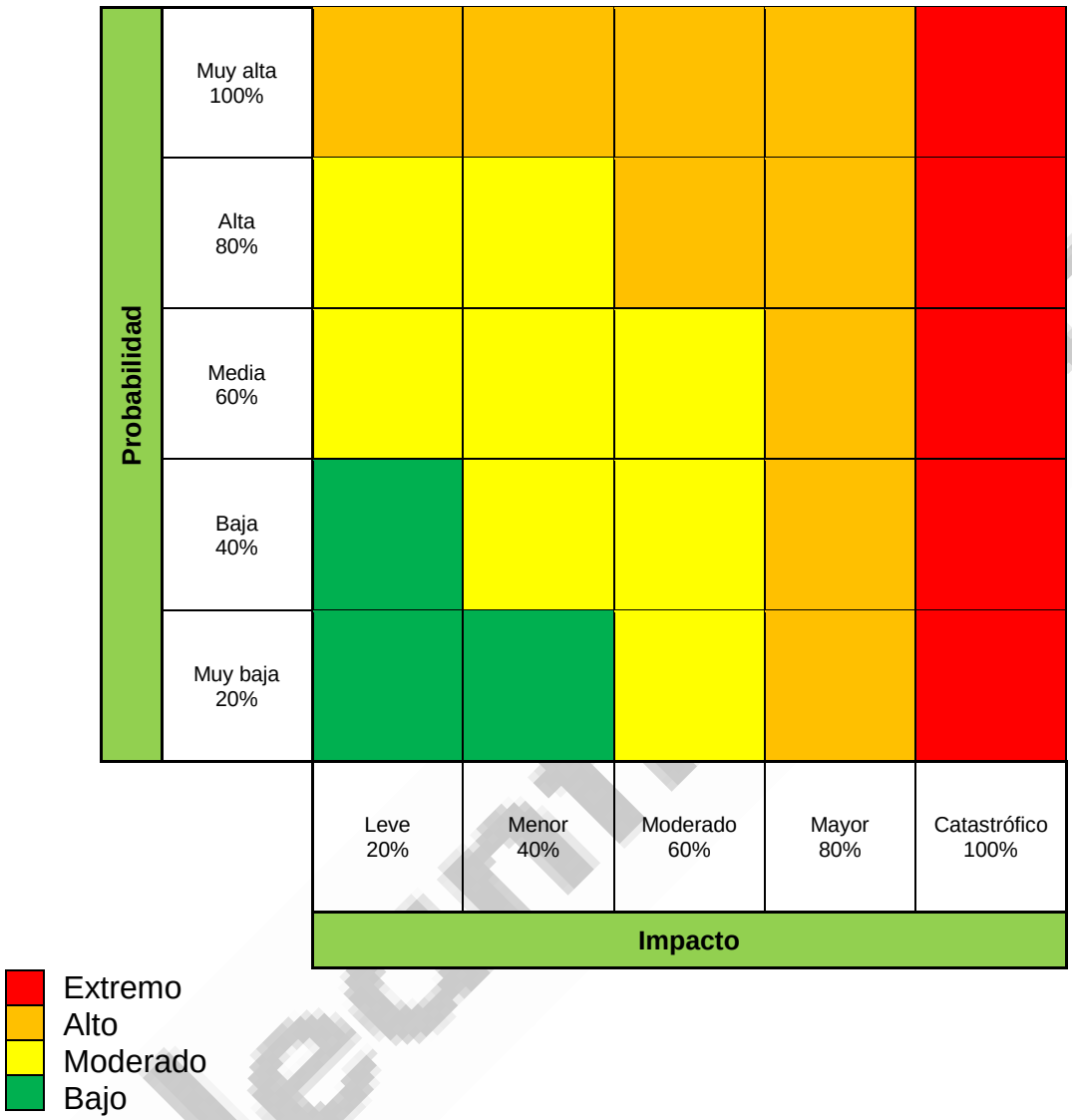
Conforme con lo anterior, en la siguiente tabla se definen los criterios para determinar el impacto (y su valoración) *para los riesgos de gestión, fiscales y de seguridad de la información*:

Nivel	Porcentaje	Tipo de afectación			
		Económica	De reputación	Legal	Operativa
Leve	20%	Menor a 10 SMLMV	Afecta la imagen de algún área de la organización.	Interposición de denuncias.	Impacta la ejecución de una tarea.
Menor	40%	Entre 10 y 50 SMLMV	Afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta administradora y/o de proveedores.	Investigaciones disciplinarias internas. Presentación de tutelas.	Impacta la ejecución de una actividad.
Moderado	60%	Entre 50 y 100 SMLMV	Afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	Investigaciones fiscales, penales o disciplinarias por parte de entes de control.	Impacta la ejecución de un procedimiento
Mayor	80%	Entre 100 y 500 SMLMV	Afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	Sanciones penales o disciplinarias.	Impacta la ejecución de un proceso, subproceso o proyecto.
Catastrófico	100%	Mayor a 500 SMLMV	Afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.	Sanciones fiscales o indemnizaciones pagadas por la Entidad.	Impacta la ejecución de varios procesos, subprocesos o proyectos de la entidad.

El *nivel de severidad o zona de riesgo inicial* (riesgo inherente) se obtiene entonces al ubicar la probabilidad y el impacto del riesgo en la matriz de severidad o *mapa de calor*.

9.3. Criterios para determinar la zona de riesgo (mapa de calor).

La matriz de severidad o mapa de calor permite determinar el nivel de severidad de un riesgo a través de la combinación de su probabilidad de ocurrencia y su impacto.



Para ello, se ubica el valor de la probabilidad en la fila y el valor del impacto en la columna correspondientes; el punto de intersección entre la fila y la columna señalará el nivel de severidad del daño (extremo, alto, moderado o bajo).

10. Lineamientos para la evaluación de riesgos.

La evaluación es el proceso mediante el cual se confrontan los resultados del análisis (riesgo inherente) con la *efectividad* de los controles existentes o establecidos en los procesos, con el fin de determinar su *nivel de severidad o zona de riesgo final* (riesgo residual).

10.1. Tipos de controles.

Los controles pueden clasificarse según el momento en que se activan en el ciclo de los procesos, o según la forma en que se ejecutan.

Según el momento en que se activan:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo; busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso, el cual detecta que algo ocurre y devuelve el proceso a los controles preventivos o a las actividades previas para su revisión. Este tipo de control detecta el riesgo, pero genera reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Este tipo de control, dado que permite reducir el impacto de la materialización del riesgo, tiene un costo asociado en su implementación.

Según la forma en que se ejecutan:

- **Control manual:** control que es ejecutado por personas, por lo cual admite implícitamente la posibilidad de error humano.
- **Control automático:** Control consistente en actividades de procesamiento o validación de información ejecutadas por un sistema o aplicativo de manera automática, sin la intervención de personas para su realización.

10.2. Criterios para valorar la efectividad de los controles.

Para cada uno de los controles identificados se debe hacer un análisis de sus características, que permita asignarle un valor a su efectividad según la siguiente tabla:

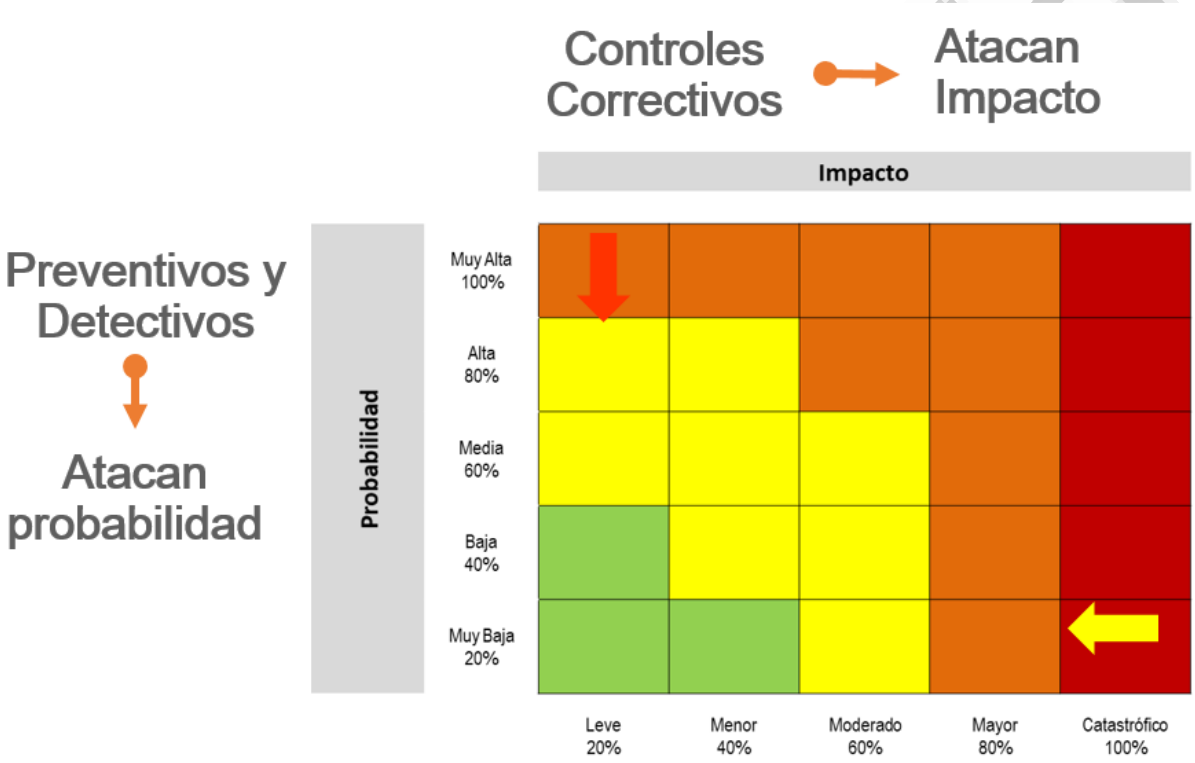
Características		Valor
Activación	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación	Automático	25%
	Manual	15%

La *efectividad total* del control estará dada por la suma de los valores de sus características de activación e implementación (*efectividad activación + efectividad implementación*).

10.3. Lineamientos para la aplicación de controles.

La aplicación de los controles producirá un desplazamiento del nivel de severidad de los riesgos en el mapa de calor; el desplazamiento será en uno de los ejes del mapa (probabilidad o impacto) según el tipo de control[7]:

✓ *Los controles **preventivos y detectivos** atacan (disminuyen) la **probabilidad**.*
✓ *Los controles **correctivos** atacan (disminuyen) el **impacto**.*



Determinar el *nivel de severidad o zona de riesgo final* (riesgo residual) para un riesgo implica calcular la probabilidad residual y el impacto residual del mismo, para ubicarlo nuevamente en el mapa de calor:

$$P_r = P_i - (P_i \times E_t)$$

$$I_r = I_i - (I_i \times E_t)$$

[7] Imagen tomada de la "***Guía para la administración del riesgo y el diseño de controles en las entidades públicas***", versión 6 (2022), Departamento Administrativo de la Función Pública (DAFP), sección 3.2.2.3. "*Análisis y evaluación de los controles*", pp. 49

Donde:
***P**r*: Probabilidad residual.
***P**i*: Probabilidad inherente (inicial) del riesgo.
***I**r*: Impacto residual.
***I**i*: Impacto inherente (inicial) del riesgo.
***E**t*: Efectividad total del control.

En la aplicación de múltiples controles se debe tener en cuenta que éstos *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 sobre el valor resultante luego de la aplicación del primer control*.

11. Apetito, tolerancia y capacidad de riesgo.

El concepto de *apetito de riesgo* se refiere al nivel de riesgo que se está dispuesto a aceptar en la búsqueda de alcanzar los objetivos. Se debería entender como *el riesgo que la entidad desea o está dispuesta a asumir, siempre y cuando esté bajo control, para lograr sus objetivos institucionales; aquel con el que se siente cómoda*.

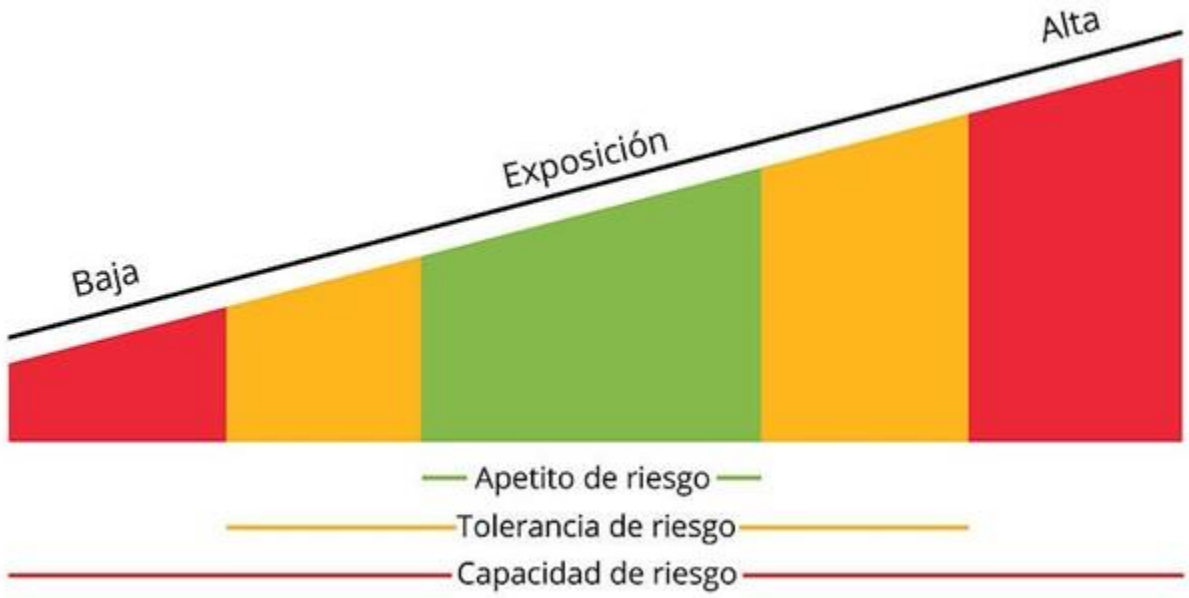
La *tolerancia al riego* es el nivel aceptable de variación del riesgo en los resultados o actuaciones de la institución relativas al logro de sus objetivos. Se refiere a *la desviación en el nivel de riesgo con respecto al apetito que, en caso de aparecer, la entidad tiene que ser capaz de soportar; sirve de alerta para evitar llegar al nivel que establece la capacidad*.

La *capacidad de riesgo es el nivel máximo de riesgo que una entidad es capaz de soportar* en la búsqueda de alcanzar sus objetivos.

Los tres conceptos son diferentes, pero están relacionados y son complementarios entre sí:
Una empresa quiere estar segura que asume el suficiente riesgo para poder conseguir sus objetivos, pero, al mismo tiempo, desea saber que no está asumiendo más riesgo del que debería, considerando los objetivos que persigue. Por ello, debe verificar que el riesgo asumido en cada momento está dentro de los límites que marca su apetito, evitando que se acerque al nivel de tolerancia establecido y, en caso de hacerlo, deberá tomar las medidas necesarias para reducir la exposición a ese riesgo lo antes posible, evitando llegar al límite marcado por su capacidad.

La relación entre estos tres conceptos se sintetiza en la siguiente imagen[8]:

[8] Imagen tomada de la guía "***Definición e implantación de apetito de riesgo***", Instituto de auditores internos de España, junio de 2013, https://auditoresinternos.es/la-f%C3%A1brica-de-pensamiento/documentos, pp. 16.



En Teleantioquia se establecen el apetito, la tolerancia y la capacidad de riesgo institucional según los valores de la siguiente tabla:

Tipo de riesgo	Apetito		Tolerancia		Capacidad	
	Probabilidad	Impacto	Probabilidad	Impacto	Probabilidad	Impacto
Gestión	50%	50%	±30% (entre 20% y 80%)	±20% (entre 30% y 70%)	90%	80%
Fiscal	50%	50%	±30% (entre 20% y 80%)	±20% (entre 30% y 70%)	90%	80%
Seguridad de la información	50%	50%	±30% (entre 20% y 80%)	±20% (entre 30% y 70%)	90%	80%
Corrupción	30%	30%	±30% (entre 0% y 60%)	±30% (entre 0% y 60%)	80%	80%

12. Lineamientos para el tratamiento del riesgo residual.

El tratamiento del riesgo es la decisión que toma la primera línea de defensa sobre cómo actuar para combatir un determinado nivel de riesgo.
Las opciones de tratamiento se analizan, *para procesos en funcionamiento, frente al nivel de riego residual*. *Para procesos nuevos se analizan a partir del nivel de riesgo inherente*.

A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, los líderes de proceso y subproceso, directores de proyecto y supervisores de contrato tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener

sobre la entidad, la probabilidad e impacto del riesgo y la relación costo beneficio de las medidas de tratamiento. En caso que una respuesta ante el riesgo derive en un nivel de riesgo residual que supere los niveles aceptables para la institución (capacidad de riesgo), se deberá analizar y revisar nuevamente dicho tratamiento.

12.1. Opciones para el tratamiento del riesgo.

Las opciones para el tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias, y pueden implicar una o más de las siguientes:

- **Aceptar el riesgo**: después de analizar y considerar los niveles del riesgo se determina asumir el mismo sin adoptar ninguna medida que modifique su probabilidad o impacto, aceptando los efectos de su posible materialización. El responsable no tiene la necesidad ni la obligación de definir planes de tratamiento o mejoramiento adicionales, pero sí de mantener en ejecución los controles existentes que permitieron lograr la mitigación inicial del riesgo. *Los riesgos de corrupción no admiten la aceptación del riesgo*.
- **Reducir el riesgo**: Tratar los riesgos para disminuir sus niveles; puede llevarse a cabo de dos formas:
  - → **Mitigar el riesgo**: después de analizar y considerar los niveles de riesgo se adoptan medidas internas encaminadas a disminuir la probabilidad o el impacto (o ambas). No necesariamente implica la creación de controles adicionales.
  - → **Compartir o transferir el riesgo**: después de realizar el análisis se considera que la mejor estrategia es reducir el impacto a través de la tercerización de la actividad o el proceso que generan el riesgo, para transferir las posibles afectaciones a otra organización; trasladar el riesgo a través de seguros o pólizas, o distribuir una porción del riesgo con otra entidad a través de medios como los contratos a riesgo compartido. La responsabilidad económica recae sobre el tercero, pero no es posible transferir la responsabilidad sobre la afectación reputacional.
- **Evitar el riesgo**: después de realizar el análisis se considera que el nivel de riesgo es demasiado alto y por tanto la mejor estrategia es *no ejecutar (abandonar)* la actividad o proceso que genera este riesgo.

12.2. Tratamiento según el nivel de severidad (zona de riesgo).

Las opciones para el tratamiento de riesgos según su nivel de severidad (zona de riesgo) a nivel institucional se definen para Teleantioquia en la siguiente tabla:

Nivel de severidad	Tipo de riesgo			
	Gestión	**Fiscal**	**Seguridad de la información**	**Corrupción**
Bajo	**<u>Aceptar el riesgo</u>**, administrándolo por medio de las actividades propias del proceso, procedimiento o actividad asociada.	**<u>Aceptar el riesgo</u>**, administrándolo por medio de las actividades propias del proceso, procedimiento o actividad asociada.	**<u>Aceptar el riesgo</u>**, administrándolo por medio de las actividades propias del proceso, procedimiento o actividad asociada.	*No existen riesgos de corrupción con nivel de severidad bajo.*
Moderado	• **<u>Aceptar el riesgo</u>** *<u>haciendo monitoreo del mismo al menos tres veces al año</u>*, si su nivel de severidad es menor o igual que el apetito de riesgo. • **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir), si su nivel de severidad es mayor que el apetito de riesgo.	• **<u>Aceptar el riesgo</u>** *<u>haciendo monitoreo del mismo al menos tres veces al año</u>*, si su nivel de severidad es menor o igual que el apetito de riesgo. • **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir), si su nivel de severidad es mayor que el apetito de riesgo.	• **<u>Aceptar el riesgo</u>** *<u>haciendo monitoreo del mismo al menos tres veces al año</u>*, si su nivel de severidad es menor o igual que el apetito de riesgo. • **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir), si su nivel de severidad es mayor que el apetito de riesgo.	• **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir).
Alto	• **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir), si su nivel de severidad es menor o igual que la tolerancia al riesgo. • **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir) *<u>haciendo monitoreo del mismo al menos tres veces al año</u>*, si su nivel de severidad es mayor que la tolerancia al riesgo y menor o igual que la capacidad de riesgo. • **<u>Compartir o transferir el riesgo</u>**, si su nivel de severidad es mayor que la capacidad de riesgo.	• **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir), si su nivel de severidad es menor o igual que la tolerancia al riesgo. • **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir) *<u>haciendo monitoreo del mismo al menos tres veces al año</u>*, si su nivel de severidad es mayor que la tolerancia al riesgo y menor o igual que la capacidad de riesgo. • **<u>Compartir o transferir el riesgo</u>**, si su nivel de severidad es mayor que la capacidad de riesgo.	• **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir), si su nivel de severidad es menor o igual que la tolerancia al riesgo. • **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir) *<u>haciendo monitoreo del mismo al menos tres veces al año</u>*, si su nivel de severidad es mayor que la tolerancia al riesgo y menor o igual que la capacidad de riesgo. **<u>Compartir o transferir el riesgo</u>**, si su nivel de severidad es mayor que la capacidad de riesgo.	• **<u>Reducir el riesgo</u>** (mitigar, compartir o transferir) *<u>haciendo monitoreo bimensual del mismo</u>*, si el nivel de severidad es menor o igual que la capacidad de riesgo. • **<u>Compartir o transferir el riesgo</u>**, si su nivel de severidad es mayor que la capacidad de riesgo.
Extremo	• **<u>Evitar el riesgo</u>**.	• **<u>Evitar el riesgo</u>**.	• **<u>Evitar el riesgo</u>**.	• **<u>Evitar el riesgo</u>**.

Cuando se seleccione la opción de reducir el riesgo (al mitigar, compartir o transferir) se debe definir un plan de acción que especifique como mínimo el responsable de ejecutarlo, la fecha de implementación y la(s) fecha(s) de seguimiento. Dicho plan deberá registrarse en el mapa o matriz de riesgos del proceso o subproceso.

13. Seguimiento, monitoreo y evaluación.

Para asegurar la eficacia y mejora continua en la gestión del riesgo, es indispensable realizar verificaciones sistemáticas para comprobar que los controles y acciones de tratamiento se comportan como estaba previsto y efectivamente disminuyen o eliminan los riesgos identificados, establecer si los factores de riesgo sufren modificaciones que alteren la probabilidad o el impacto de los mismos, y determinar si los lineamientos y metodología empleados se mantienen vigentes frente a cambios en el entorno.

En consideración a lo anterior, en la siguiente tabla se definen las acciones de seguimiento, monitoreo y evaluación frente a los diferentes elementos integrantes de la gestión del riesgo, así como sus periodos de ejecución y responsables:

Responsable		Acción	Periodicidad
Línea estratégica	**Alta dirección**[9]: • Gerente • Secretario general • Directores • Líderes de área • Jefes • Coordinadores que dependen del Gerente	Seguimiento a los niveles de aceptación de los riesgos, así como al apetito, tolerancia y capacidad del riesgo del canal. Definición y ajuste de los lineamientos generales para la administración del riesgo.	Mínimo una vez cada dos años
		Seguimiento y supervisión a la gestión de los riesgos institucionales.	Anual
	Comité institucional de coordinación de control interno (CICCI)	Revisar, aprobar y evaluar la política de administración de riesgos.	Mínimo una vez cada dos años
		Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones para el fortalecimiento de la gestión del riesgo.	Mínimo una vez al año
	Comité institucional de gestión y desempeño (CIGD)	Revisar el contexto estratégico, plataforma estratégica, el modelo de operación por procesos y la planeación institucional, con el fin de analizar los posibles eventos de riesgos que se puedan materializar en el ejercicio de la labor misional.	Mínimo una vez cada dos años
		Analizar, evaluar y aprobar el mapa de riesgos institucional, y las actualizaciones del mismo.	Anual
Primera línea	• Líderes de proceso • Líderes de subproceso • Directores de proyecto • Supervisores de contratos	Identificar y valorar los riesgos y controles de los procesos, subprocesos, proyectos y contratos bajo su responsabilidad, con la participación de su equipo de trabajo.	Anual
		Implementar los controles identificados no existentes previamente en los procesos, subprocesos, proyectos y contratos bajo su responsabilidad.	Anual
		Monitorear los controles implementados en los procesos, subprocesos, proyectos y contratos bajo su responsabilidad.	Mínimo tres veces al año
		Realizar seguimiento y análisis a los controles de los riesgos, buscando detectar las deficiencias de estos, para determinar las acciones de mejora requeridas.	Mínimo tres veces al año
Segunda línea	Oficina de planeación	Revisar y evaluar la metodología para la identificación, análisis, valoración y evaluación del riesgo.	Mínimo una vez cada dos años
		Monitorear los controles y procesos de gestión de riesgos de la primera línea, para asegurar que son apropiados y funcionan correctamente.	Mínimo dos veces al año
		Consolidar el Mapa de riesgos institucional, presentarlo para su análisis, evaluación y aprobación ante el Comité Institucional de Gestión y Desempeño y publicarlo conforme a los lineamientos normativos.	Anual
		Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio.	Mínimo una vez cada dos años
	• Secretario general • Directores • Líderes de área • Jefes	Supervisar que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos, en cumplimiento de los lineamientos para la gestión de riesgos.	Mínimo una vez al año

[9] Ver Nota 3.

Responsable		Acción	Periodicidad
	• Coordinadores	Realizar seguimiento al mapa de riesgos de su área.	Mínimo dos veces al año
		Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad.	Mínimo una vez cada dos años
		Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico (secretario general).	Mínimo una vez al año
		Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo.	Mínimo una vez al año
Tercera línea	Oficina de control interno	Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.	Mínimo una vez al año
		Presentar al Comité Institucional de Coordinación de Control Interno el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria.	Mínimo tres veces al año
		Evaluar la eficacia, eficiencia y efectividad de los controles en los mapas de riesgos, y sus debilidades.	Mínimo una vez al año

Adicionalmente deben cumplirse los seguimientos establecidos en los diferentes planes de acción y los monitoreos definidos en las opciones de tratamiento de riesgos.

14. Lineamientos para actuar frente a la materialización de riesgos.

En la eventualidad de llegarse a materializar un riesgo, se deberán emprender las acciones relacionadas a continuación:

Responsable	Acción	
	Riesgos de gestión/fiscales/seguridad de la información	Riesgos de corrupción
• Líderes de proceso • Líderes de subproceso • Directores de proyecto • Supervisores de contratos	– Informar a la oficina de planeación y a la de control interno sobre el riesgo materializado. – Proceder de manera inmediata con las acciones correctivas necesarias para mitigar el impacto. – Iniciar el análisis de causas para determinar las acciones preventivas y de mejora que se requieran para evitar su repetición. – Construir y documentar el plan de mejoramiento, incluyendo las acciones correctivas, preventivas y de mejora determinadas. – Revisar y replantear los riesgos del proceso, subproceso, proyecto o contrato, y actualizar el mapa de riesgos.	– Informar a la oficina de planeación, la oficina de control interno y la secretaría general sobre el hecho encontrado, a fin de determinar las acciones que se deben tomar. – Una vez surtido el conducto regular establecido por la entidad, y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. – Proceder de manera inmediata con las acciones correctivas necesarias para mitigar el impacto. – Iniciar el análisis de causas para determinar las acciones preventivas y de mejora que se requieran para evitar su repetición. – Construir y documentar el plan de mejoramiento, incluyendo las acciones correctivas, preventivas y de mejora determinadas. – Revisar y replantear los riesgos del proceso, subproceso, proyecto o contrato, y actualizar el mapa de riesgos.
Oficina de control interno	– Informar al líder del proceso o subproceso, director de proyecto o supervisor de contrato acerca del hecho encontrado.	– Informar al líder del proceso o subproceso, director de proyecto o supervisor de contrato acerca del hecho encontrado. – Informar a la oficina de planeación y a la secretaría general con el fin de facilitar el inicio de las

Responsable	Acción	
	Riesgos de gestión/fiscales/seguridad de la información	Riesgos de corrupción
	– Informar a la oficina de planeación con el fin de facilitar el inicio de las acciones correspondientes para revisar y actualizar el mapa de riesgos. – Acompañar al líder del proceso o subproceso, director de proyecto o supervisor de contrato en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. – Verificar que se tomaron las acciones necesarias y se actualizó el mapa de riesgos correspondiente.	acciones correspondientes con el líder del proceso o subproceso, director de proyecto o supervisor de contrato, y para revisar y actualizar el mapa de riesgos. – Acompañar al líder del proceso o subproceso, director de proyecto o supervisor de contrato en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. – Verificar que se tomaron las acciones necesarias y se actualizó el mapa de riesgos correspondiente.
Comité institucional de coordinación de control interno (CICCI)	– Analizar las causas de los eventos (riesgos materializados) y definir cursos de acción para prevenir su repetición futura.	