ANEXO

POLÍTICA Y METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS DE CORPOCALDAS

Corpocaldas

CORPORACION AUTONOMA REGIONAL DE CALDAS

ANEXO

POLÍTICA Y METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS DE CORPOCALDAS

Versión 2

Manizales, diciembre de 2024

POLÍTICA Y METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS DE CORPOCALDAS

Proceso: Mejora Contina

Aprobadores

Aprobó	Reviso	Elaboro
Comité Institucional de Coordinación de Control Interno Acta No. 07 de 9 de octubre del 2024	Subdirector de Planificación Ambiental del Territorio Wilford Rincon Arango	Equipo de Mejora continua: Luz Piedad Gonzalez Gerardo Giraldo Ricardo Alarcón Enlace del SGI: German Guillermo Murillo Jefe de control interno: Lina Maria Daza Jefe de control disciplinario: Carolina Zapata

CONTENIDO

1. INTRODUCCION 7
2. GLOSARIO 9
3. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS 17
4. OBJETIVO DE LA POLITICA DE RIESGOS 8
5. ALCANCE 8
6. NIVELES DE RESPONSABILIDAD Y COMPROMISOS PARA EL MANEJO DE LOS RIESGOS 19
7. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS 21
7.1. Nivel de calificación de probabilidad para riesgos de proceso y seguridad de la información ..... **¡Error! Marcador no definido.**
7.2. Nivel de calificación de probabilidad para riesgos de corrupción **¡Error! Marcador no definido.**
7.3. Niveles de calificación de impacto de riesgos de procesos y seguridad de la información ..... **¡Error! Marcador no definido.**
7.4. Calificación de impacto para riesgos de corrupción **¡Error! Marcador no definido.**
8. TRATAMIENTO Y MANEJO PARA LOS RIESGOS SEGÚN EL NIVEL DE SEVERIDAD 34
9. ESTRATEGIAS DE SEGUIMIENTO Y MONITOREO AL MAPA DE RIESGOS (SEGÚN RESPONSABILIDADES DE LAS LINEAS DE DEFENSA) 35
Tipo de Riesgo 35
Zona de Riesgo Residual ..... **¡Error! Marcador no definido.**
Estrategia de Tratamiento – Controles 35
Riesgos de Gestión y Seguridad de la información ..... **¡Error! Marcador no definido.**
Baja ..... **¡Error! Marcador no definido.**
Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en el módulo de riesgos- SGI. ..... **¡Error! Marcador no definido.**
Moderada ..... **¡Error! Marcador no definido.**

Se realiza seguimiento a los controles con periodicidad TRIMESTRAL y se registran sus avances en el módulo de riesgos- SGI. ..... **¡Error! Marcador no definido.**

Alta ..... **¡Error! Marcador no definido.**

Extrema ..... **¡Error! Marcador no definido.**

Riesgos de Corrupción 35

Para todos los riesgos de corrupción se realiza seguimiento TRIMESTRAL y se registra en el módulo de riesgos – SGI. 35

La oficina de Control interno realiza seguimiento CUATRIMESTRAL ..... **¡Error! Marcador no definido.**

10. ACCIONES FRENTE A DESVIACIONES EN LA APLICACIÓN DE LOS CONTROLES 37

11. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS 38

12. DIVULGACION 39

13. CAPACITACION 39

14. ANEXO 1 GOBIERNO DEL RIESGO.....15

15. ANEXO 2 CULTURA DEL RIESGO.....15

ÍNDICE DE TABLAS

Tabla 1. Modelo de las tres líneas de defensa, roles y responsabilidades en Corpocaldas 19
Tabla 2. Clasificación de los riesgos. 21
Tabla 3. Niveles de aceptación al riesgo. 22
Tabla 4. Definición del riesgo de corrupción - ejemplo aplicado con concurrencia de componentes 25
Tabla 5. Criterios para definir la probabilidad en riesgos de gestión, fiscales y seguridad de la información. 28
Tabla 6. Criterios para definir la probabilidad en riesgos de corrupción 29
Tabla 7. Criterios para definir el impacto en riesgos de gestión, fiscales y de seguridad de la información 29
Tabla 8. Criterios para calificar el impacto riesgos de corrupción 31
Tabla 9. Estrategias de seguimiento y monitoreo al mapa de riesgos de la Corporación. 35
Tabla 10. Temáticas asociadas a los controles 37
Tabla 11. Descripción de acciones y responsables ante riesgos materializados 38

ÍNDICE DE FIGURAS

Ilustración 1. Metodología para la Administración del Riesgo 23
Ilustración 2. Matriz de calor (niveles de severidad del riesgo) 32
Ilustración 3. Mapa a de calor para establecer el nivel del riesgo inherente. 33
Ilustración 4. Opciones de tratamiento de los riesgos 34

1. INTRODUCCION

La Política de Administración del Riesgo para la Corporación Autónoma Regional de Caldas, contiene los lineamientos para la administración de los riesgos de gestión, fiscales, corrupción y seguridad de la información, tomando como referencia las directrices de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública DAFP y el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del Ministerio de Tecnologías de la Información y Comunicaciones – MinTic, las cuales sirven de base para asegurar el cumplimiento de la misión institucional y los objetivos estratégicos de la Corporación.

Así mismo el Modelo Integrado de Planeación y Gestión - MIPG busca articular El Sistema De Gestión con el Sistema de Control Interno a partir de la implementación de las 7 dimensiones, en especial la de control interno, la cual promueve el mejoramiento continuo y se establecen las acciones, métodos y procedimientos de control y de gestión del riesgo para las entidades públicas y desarrolla una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua.

Con lo anterior la Corporación cuenta con la Política y Metodología de Administración del Riesgo la cual busca establecer criterios orientadores para la identificación, análisis, valoración y tratamiento de los posibles eventos a través de una cultura organizacional fundamentada en la prevención, la información, el control, y la evaluación, para la toma de decisiones, la mejora continua y el cumplimiento de los objetivos estratégicos de la entidad.

2. OBJETIVO DE LA POLITICA DE RIESGOS

Definir la Política y Metodología para la Administración del Riesgo con el fin de emprender las medidas necesarias y establecer criterios orientadores para la identificación, análisis, valoración y tratamiento de los posibles eventos que se puedan presentar en el desarrollo de la gestión institucional y su normal operación, en donde cada servidor se constituya como parte integral de la gestión del riesgo, a través de una cultura organizacional fundamentada en la prevención, la información, el control, y la evaluación, para la toma de decisiones, la mejora continua y el cumplimiento de los objetivos estratégicos de la entidad.

2.1. Objetivos específicos

- Definir las metodologías para la administración de los diferentes tipos de riesgo.
- Establecer las responsabilidades en la administración de los riesgos.
- Direccionar la cultura organizacional, en función del desarrollo de un pensamiento basado en riesgos.
- Definir estrategias de comunicación y divulgación adecuadas para la apropiación de la administración del riesgo en la Corporación.

3. ALCANCE

La Política de Administración del Riesgo es aplicable a toda la Corporación de acuerdo con su estructura organizacional y gestionada por el personal

de la entidad a través de la operación por procesos estratégicos, misionales, apoyo y de evaluación en los niveles del modelo de las líneas de defensa.

4. GLOSARIO

- **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.
- **Aceptación del riesgo:** Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
- **Administración del Riesgo:** Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.
- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis de Riesgos**: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.
- **Apetito al riesgo**: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. (Guía para la administración del riesgo y el diseño de controles en entidades públicas V5, 2020, págs. 24)
- **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.

- **CICCI:** Comité Institucional de Coordinación de control Interno.
- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, 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.
- **Control:** Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.
- **Control detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **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 automático:** Son ejecutados por un sistema.
- **Control manual:** Controles que son ejecutados por personas.
- **Compartir el riesgo:** Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Evaluación del riesgo**: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo y su magnitud o ambos son aceptables o tolerables.
- **Factores de Riesgo:** Fuente generadora de los eventos de riesgos

operativos.

- **Gestión del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

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

- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales. 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.

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

- **Identificación del riesgo:** Proceso de análisis para encontrar una

potencial desviación de los objetivos.

- **Impacto:** Se entiende como las consecuencias que pueden 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. 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.
- **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).
- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.
- **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 por Impacto, sin embargo, pueden

relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **Plan Anticorrupción y de Atención al Ciudadano**: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.
- **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.
- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

  Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el

recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos

- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **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 Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital, puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **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.
- **Riesgo inherente:** Es aquel riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo permanente luego de tomar medidas de tratamiento del riesgo.
- **Tolerancia al riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad. Para el riesgo de corrupción la tolerancia es inaceptable.

- **Vulnerabilidad:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
- **Tratamiento del riesgo:** Consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.
- **Valoración del riesgo:** Busca identificar y analizar los riesgos que enfrenta la entidad, tanto de fuentes internas como externas relevantes para la consecución de los objetivos, para administrarlos.

5. MARCO NORMATIVO

- Decreto 1078 del 2015 "Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones".
- Decreto 1083 del 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública".
- Decreto 1499 del 11 de septiembre del 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".
- Resolución 2457 de 2017, "Por la cual se establece la Política y Metodología para la Administración del Riesgo en la Corporación Autónoma Regional de Caldas.
- Decreto 648 de 2017, Por la cual establece, como una de las funciones del Comité Institucional de Coordinación de Control Interno, someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.
- Resolución 2335 de 2021 "Por la cual se actualiza y adopta la Política y Metodología para la Administración de Riesgos de la Corporación Autónoma Regional de Caldas".
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022.
- Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG) – Versión 5 – marzo 2023.

6. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Política de Administración de Riesgos de la Corporación tiene un carácter estratégico y está fundamentada en el Modelo Integrado de Planeación y Gestión, la Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

- **Los riesgos de gestión de proceso** que puedan afectar el cumplimiento de la misión y los objetivos institucionales y estratégicos de la entidad.
- **Los riesgos de posibles actos de corrupción** a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Los riesgos de seguridad de la información** que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.
- **Riesgos fiscales** que puedan producir un efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

7. NIVELES DE RESPONSABILIDAD Y COMPROMISOS PARA EL MANEJO DE LOS RIESGOS

La responsabilidad frente a la administración del riesgo en Corpocaldas, está definida mediante el modelo de las tres líneas de defensa del IIA – 2020 (The Institute of Internal Auditors) y la entidad lo acoge según tabla 1.

Tabla 1. Modelo de las tres líneas de defensa, roles y responsabilidades en Corpocaldas

LÍNEAS DE DEFENSA	ROLES (NIVELES DE AUTORIDAD)	RESPONSABILIDADES GENERALES
Línea Estratégica	• Comité Directivo • Comité Institucional de Coordinación de Control Interno.	Responsable de definir, revisar, validar y supervisar el cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimiento a la gestión y auditoría interna para toda la entidad. A esta línea debe subir el análisis de eventos y riesgos críticos.
Primera Línea de Defensa	• Coordinadores • Líderes de procesos • Todos los funcionarios que tienen una responsabilidad frente a la aplicación de controles.	Responsables de gestionar los riesgos, realizar seguimiento permanente a los riesgos y a la aplicación de controles y reporte de eventos materializados.

LÍNEAS DE DEFENSA	ROLES (NIVELES DE AUTORIDAD)	RESPONSABILIDADES GENERALES
Segunda Línea de Defensa	• Subdirección de Planificación • Líderes de Sistemas de Gestión • Comité Institucional de Gestión y Desempeño • Gestores de Riesgos o Comité de Riesgos.	Liderar los sistemas de gestión de riesgos, acompañar el proceso, asegurar su cumplimiento, realizar seguimiento y control efectivo a la aplicación de las medidas de tratamiento, revisar los riesgos materializados. Hace seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos. Capacita, asesora, acompaña y define metodología.
Tercera Línea de Defensa	• Oficina de Control Interno. • Revisoría Fiscal.	Aplicar procesos de seguimiento y evaluación a través de la auditoría interna y externa, para establecer la efectividad de los controles y evitar la materialización de riesgos. Evalúa de manera independiente y objetiva los controles de la segunda línea de defensa para asegurar su objetividad y cobertura; así mismo evalúa los controles de primera línea de defensa que no se encuentren cubiertos o inadecuadamente cubiertos por la segunda línea de defensa.

Fuente: Corpocaldas, elaboración propia, agosto de 2024.

8. CLASIFICACIÓN DEL RIESGO

Los riesgos en la Corporación Autónoma Regional de Caldas - Corpocaldas, se clasifican según las tipologías descritas en la siguiente tabla.

Tabla 2. Clasificación de los riesgos.

CLASIFICACIÓN	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la Corporación, en las cuales está involucrado por lo menos un participante interno de la entidad y en donde prevalece la intencionalidad y/o el ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, contratación, 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
Legales	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la entidad debido a su incumplimiento o desacato a la normativa vigente
Estratégicos	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la Corporación y por tanto impactan toda la entidad.
Sistemas de Gestión	Posibilidad de ocurrencia de eventos que afecten la implementación, operación, mantenimiento y sostenibilidad de los Sistemas de Gestión que conforman el Sistema Integrado de Gestión - SIG
Pérdida de confidencialidad	Pérdida de la propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Pérdida de integridad	Pérdida de la propiedad de exactitud y completitud de la información.
Pérdida de disponibilidad	Pérdida de la propiedad de la información de ser accesible y utilizable a demanda por la entidad.
Riesgos de corrupción	Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Conflicto de intereses	Posibilidad de que una situación producida por un interés particular pueda influir o sesgar el juicio/decisión de un servidor público contratista en el ejercicio de sus funciones u obligaciones contractuales.
Riesgos fiscales	Efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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

9. APETITO DE RIESGO

Corresponde al nivel de riesgo que la Corporación esta dispuesto o no a aceptar en relación con sus objetivos, el marco legal y las disposiciones de la Alta Dirección.

Para los riesgos de gestión y de seguridad de la información, en la tabla 3, se establecen los siguientes niveles de aceptación al riesgo.

Tabla 3. Niveles de aceptación al riesgo.

NIVEL DE RIESGO RESIDUAL	NIVEL DE ACEPTACIÓN	DESCRIPCIÓN
Extremo	**No admisibles**	Los riesgos ubicados en estos niveles se considerarán como no admisibles, por lo cual se deben implementar acciones de tratamiento adicionales que permitan REDUCIR, TRANSFERIR o EVITAR el riesgo. No necesariamente es un control adicional, puede ser la mejora a un control existente. Estos riesgos deben ponerse en conocimiento de la línea estratégica: Comité Institucional de Coordinación de Control Interno.
Alto		
Moderado	**Tolerable (máxima desviación admisible)**	Los riesgos ubicados en estos niveles pueden ser tolerados por la entidad conociendo los efectos de su posible materialización, sin necesidad de implementar acciones adicionales a los controles establecidos.
Bajo	**Aceptable**	

Fuente: Elaboración propia, basada en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6 de 2022, Función Pública

Para los riesgos de corrupción y fiscales, la Corporación **no admite aceptación, ni tolerancia**, siempre deben conducir a un tratamiento (plan de acción) y requieren de un monitoreo por parte de la primera y segunda línea.

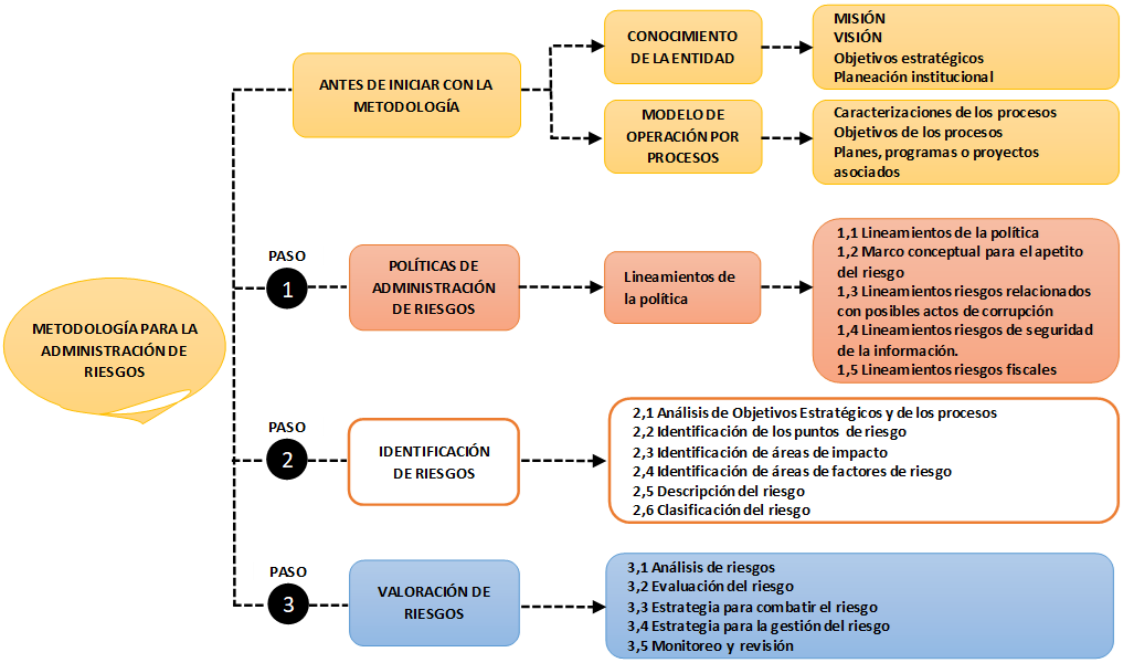
10. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS

A continuación, se describe la metodología apropiada por Corpocaldas para la administración de riesgos, la cual se basa en la versión 6 de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades

Públicas, expedida por el Departamento Administrativo de la Función Pública — DAFP del año 2022.

Se incluyen los siguientes pasos y lineamientos para administrar los riesgos de gestión, fiscales, corrupción y seguridad de la información de la siguiente manera:

Ilustración 1. Metodología para la Administración del Riesgo



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

11. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se establecen las etapas principales para la gestión de los riesgos en Corpocaldas:

11.1. Identificación del riesgo

Esta etapa tiene como objetivo identificar los riesgos y oportunidades que están bajo el control de la Corporación, para ello se deben tener en cuenta los objetivos estratégicos, la caracterización de cada proceso que contempla su objetivo y alcance y también, el análisis frente a situaciones internas y externas que pueden generar riesgos que afecten el cumplimiento de los objetivos definidos por la entidad.

- **Impacto:** Se define ¿Qué puede pasar? Los factores de impacto a los que puede estar expuesta la Corporación, son:

  - Afectación Económica: afectación presupuestal de la entidad.
  - Afectación Reputacional: afectación de la imagen de la entidad.

- **Causa inmediata:** Responde al ¿Cómo puede pasar? Son las situaciones o causas más evidentes por las cuales se puede materializar el riesgo, pero no constituyen la causa principal o base para que este se presente.

- **Causa raíz:** Da respuesta al ¿Por qué puede pasar? Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas. Esta es la base para la definición de los controles.

11.1.1. Riesgos de corrupción

Un riesgo de corrupción es 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 (Documento CONPES Número 16).

Los riesgos de corrupción se establecen sobre procesos y trámites. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos. Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones con las otras tipologías, es necesario que en la descripción del riesgo concurran los componentes de su definición según lo señalado en la siguiente tabla.

Tabla 4. Definición del riesgo de corrupción - ejemplo aplicado con concurrencia de componentes

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Riesgo de corrupción	X	X	X	X

Redacción inicia con:	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de	recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros	por el ejercicio de una función u obligación administrativa dada la concentración del poder	para la adjudicación de un contrato a un oferente en particular	

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

11.1.2. Riesgos fiscales

Estos riesgos se basan en el efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

- **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 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.

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) **+** Efecto dañoso

11.1.3. Riesgos de seguridad de la información

Estos riesgos se basan en la afectación de tres criterios en un activo de información o un grupo de activos de información, dentro de lo que se denomina como triada de la información: integridad, confidencialidad o disponibilidad.

Para cada riesgo identificado se deben asociar el grupo de activos de información o activos de información específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario tener en cuenta el Manual TIC-MN-03 Sistema de Gestión de Seguridad de la Información – SGSI, la Guía TIC-MN-03-GI-03 Gestión de Activos de Información; así como también consultar y tener en cuenta los lineamientos definidos en el "Anexo 4. Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas", el cual hace parte de los anexos de la Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, versión 6, diciembre de 2022.

11.1.4. Riesgos de gestión

Estos riesgos se basan en el 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.

Los riesgos de gestión se establecen sobre los puntos de riesgo identificados en el flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

11.2. ANÁLISIS DEL RIESGO

En esta etapa se determina la probabilidad de ocurrencia del riesgo u oportunidad y sus consecuencias, con el fin de establecer el nivel de riesgo inicial (riesgo inherente). Este análisis se efectúa posterior a la identificación del riesgo y se debe realizar aplicando los criterios para medir la probabilidad y el impacto señalados a continuación:

11.2.1. Probabilidad para riesgos de gestión, fiscales y seguridad de la información.

Se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo? La probabilidad de ocurrencia está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente corresponde al número de veces que se pasa por el punto de riesgo en el período de 1 año (frecuencia con la que se lleva a cabo una actividad en 1 año), según como se presenta en la tabla 5.

Tabla 5. Criterios para definir la probabilidad en riesgos de gestión, fiscales y seguridad de la información.

FRECUENCIA DE LA ACTIVIDAD*	NIVEL	PROBABILIDAD
La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	MUY BAJA	20%
La actividad que conlleva el riesgo se ejecuta 3 a 24 veces por año	BAJA	40%
La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	MEDIA	60%
La actividad que conlleva el riesgo se ejecuta mínimo 500 veces por año y máximo 5000 veces por año	ALTA	80%
La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	MUY ALTA	100%

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

* En materia de tecnología (incluye disponibilidad de aplicativos) se debe tener en cuenta que 1 hora de funcionamiento = 1 vez.

11.2.2. Probabilidad para riesgos de corrupción

Se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo? La probabilidad de ocurrencia está asociada a hechos que se han materializado o frente a los cuales se cuenta con un historial de situaciones o eventos asociados al riesgo, según como se muestra en la tabla 6.

Tabla 6. Criterios para definir la probabilidad en riesgos de corrupción

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
4	PROBABLE	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	POSIBLE	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
2	IMPROBABLE	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	RARA VEZ	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

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

11.2.3. Impacto para riesgos de gestión, fiscales y seguridad de la información.

Las variables principales que se tienen en cuenta para determinar el impacto (consecuencia) ante la materialización de un riesgo son los impactos económicos y reputacionales, según se presenta en la tabla 7. Cuando se presenten ambos impactos para un mismo riesgo, tanto económico como reputacional, con diferentes niveles, se debe tomar el nivel más alto.

Tabla 7. Criterios para definir el impacto en riesgos de gestión, fiscales y de seguridad de la información

NIVEL	AFECTACION REPUTACIONAL	AFECTACIÓN ECONÓMICA	CONTINUIDAD DE LA OPERACIÓN PARA RIESGOS DE S.I.
LEVE 20%	El riesgo afecta la imagen de algún área de la Corporación.	Afectación menor a 10 SMLMV	Afectación mínima en la continuidad de la operación

NIVEL	AFECTACION REPUTACIONAL	AFECTACIÓN ECONÓMICA	CONTINUIDAD DE LA OPERACIÓN PARA RIESGOS DE S.I.
MENOR 40%	El riesgo afecta la imagen de la Corporación internamente, de conocimiento general a nivel interno, de junta directiva y/o de proveedores.	Entre 10 y 50 SMLMV	Afectación mínima en la continuidad de la operación
MODERADO 60%	El riesgo afecta la imagen de la Corporación por retrasos en la prestación del servicio a los usuarios o ciudadanos, afectando el logro de los objetivos.	Entre 50 y 100 SMLMV	Puede causar interrupciones significativas en la continuidad de la operación
MAYOR 80%	El riesgo afecta la imagen de la Corporación con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal, generando reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.	Entre 100 y 500 SMLMV	Puede ocasionar una interrupción grave en la continuidad de la operación.
CATASTRÓFICO 100%	El riesgo afecta la imagen de la Corporación a nivel nacional, con efecto publicitario sostenido a nivel país.	Mayor a 500 SMLMV	

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

11.2.4. Impacto para riesgos de corrupción

Para este tipo de riesgos se tienen en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos y no pueden ser aceptados; lo anterior, teniendo en cuenta los criterios definidos en la tabla 8.

Tabla 8. Criterios para calificar el impacto riesgos de corrupción

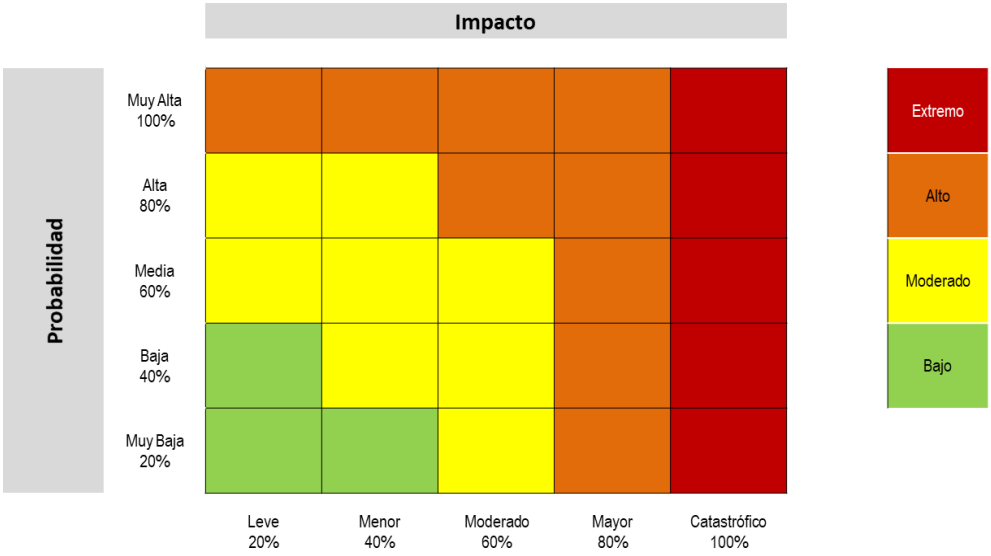
No.	Pregunta: Si es riesgo de corrupción se materializa podría:	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar al cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la Entidad?		
4	¿Afectar el cumplimento la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de los servicios?		
8	¿Dar lugar al detrimento de la calidad de vida de la comunidad por la pérdida del bien, servicio o recursos públicos?		
9	¿Generar perdida de la información de la entidad?		
10	¿Generar intervención de los órganos de control, dela Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios7		
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 vidashumanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas (s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntar (s) genera un impacto mayor Responder afirmativamente de DOCE a DIECINUEVE preguntas (s) genera un impacto catastrófico.		10	
Moderado	Genera a medianas consecuencias sobre la entidad		
Mayor	Genera altas consecuencias sobre la entidad		
Catast	Genera consecuencias desastrosas para la entidad		

No.	Pregunta: Si es riesgo de corrupción se materializa podría:	RESPUESTA	
		SI	NO
rófico			

Fuente: Guía para la Administración del Riesgo y el Diseño de controles en Entidades Públicas, DAFP, versión 6, 2022

Teniendo en cuenta los niveles de probabilidad e impacto definidos anteriormente, para los riesgos de gestión, fiscales y seguridad de la información, se definen 4 niveles de severidad en la matriz de calor, como se muestra en la ilustración 2.

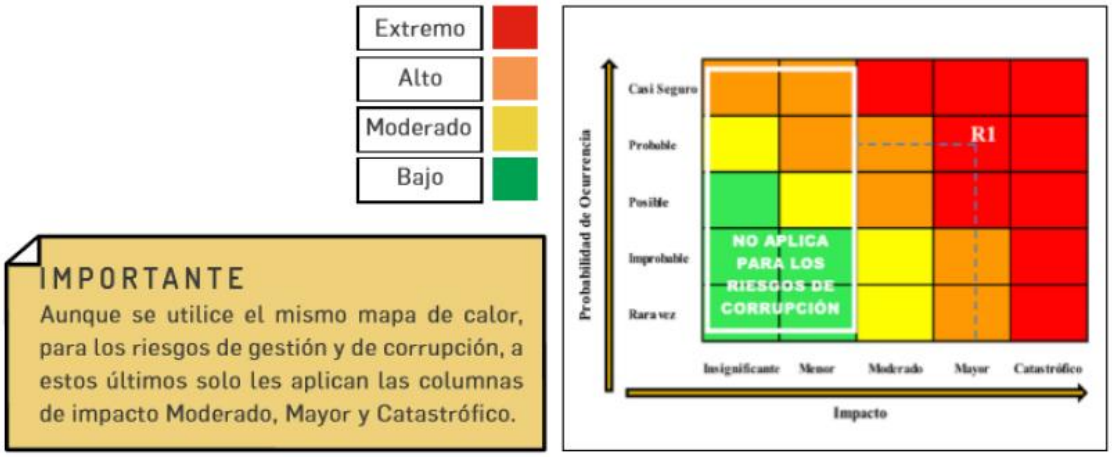
Ilustración 2. Matriz de calor (niveles de severidad del riesgo)



Fuente: Guía para la Administración del Riesgo y el Diseño de controles en Entidades Públicas, DAFP, versión 6, 2022

En el caso de los riesgos de corrupción, se definen 3 zonas o niveles de severidad en la matriz de calor, teniendo en cuenta que en el impacto solamente aplican los niveles "moderado", "mayor" y "catastrófico", como se indica en la ilustración 3.

Ilustración 3. Mapa a de calor para establecer el nivel del riesgo inherente.



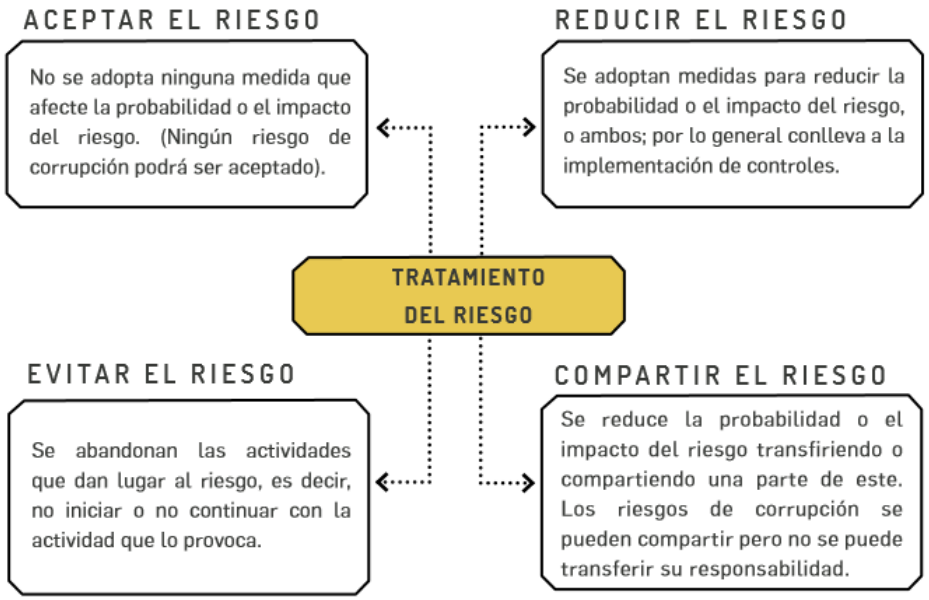
Fuente: Guía para la Administración del Riesgo y el Diseño de controles en Entidades Públicas, DAFP, versión 6, 2022

Una vez se obtenga el impacto y la probabilidad para cada riesgo identificado, se ubican las calificaciones respectivas en la fila y columna correspondientes sobre las matrices de calor de las figuras 2 o 3, según corresponda, y se establece el punto de intersección entre ambas, el cual corresponde a la zona o nivel de riesgo inicial (riesgo inherente); es decir, el riesgo que enfrenta la Corporación en ausencia de controles.

12. TRATAMIENTO Y MANEJO PARA LOS RIESGOS SEGÚN EL NIVEL DE SEVERIDAD

Las opciones para el tratamiento de los riesgos se establecen según el siguiente diagrama:

Ilustración 4. Opciones de tratamiento de los riesgos



Fuente: Guía para la Administración del Riesgo y el Diseño de controles en Entidades Públicas, DAFP, versión 6, 2022

De acuerdo con los niveles de severidad del riesgo se establece el siguiente manejo:

BAJO	Aceptar el riesgo
MODERADO	Aceptar o reducir el riesgo
ALTO	Reducir, evitar, compartir el riesgo
EXTREMO	Evitar, reducir, compartir el riesgo

Nota: Ningún riesgo de corrupción podrá ser aceptado.

13. ESTRATEGIAS DE SEGUIMIENTO Y MONITOREO AL MAPA DE RIESGOS (SEGÚN RESPONSABILIDADES DEL MODELO DE LAS TRES LINEAS)

Corpocaldas, cuenta con un módulo de riesgos dentro de aplicativo del Sistema de Gestión Integrado-SGI, a través del cual puede identificar, valorar, evaluar, administrar y realizar seguimiento a los riesgos de gestión, de corrupción, de seguridad de la información y fiscales según las responsabilidades establecidas en las líneas de defensa. Para esta labor cuenta con el apoyo de la subdirección de planificación del territorio, quién identifica los requerimientos funcionales, revisa su adecuado funcionamiento y brinda acompañamiento y asesoría a todos los funcionarios de la entidad en cargue de información.

Tabla 9. Estrategias de seguimiento y monitoreo al mapa de riesgos de la Corporación.

TIPO DE RIESGO	ESTRATEGIA DE SEGUIMIENTO Y MONITOREO
Riesgos de Corrupción y fiscales	**Línea Estratégica** - **Comité Institucional de Coordinación de Control Interno:** realizan seguimiento a los eventos materializados y a los riesgos en zona residual alta y extrema. **Primera Línea de Defensa** - **Lideres de procesos:** realizan seguimiento a los riesgos y reporte de eventos materializados. - **Coordinadores y lideres de subprocesos:** realizan seguimiento cuatrimestral a los riesgos, a la aplicación de controles y reporte de eventos materializados. - **Funcionarios que tienen una responsabilidad frente a la aplicación de controles**: registrar las evidencias de la aplicación del control en el módulo de riesgos- del Sistema de Gestión Integral según la periodicidad establecida en el mismo.

TIPO DE RIESGO	ESTRATEGIA DE SEGUIMIENTO Y MONITOREO
	Segunda Línea de Defensa - **Subdirección de Planificación Ambiental:** realizan seguimiento a las medidas de tratamiento de los riesgos. - **Comité de riesgos:** realizan seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos. **Tercera Línea de Defensa** - **Oficina de Control Interno:** realizan seguimiento cuatrimestral a los riesgos de corrupción y evaluación a la efectividad de los controles para evitar su materialización.

Fuente: Elaboración propia, Corpocaldas, diciembre de 2024.

14. ACCIONES FRENTE A DESVIACIONES EN LA APLICACIÓN DE LOS CONTROLES

Tabla 10. Temáticas asociadas a los controles

GESTIÓN	Evaluación de desempeño
	Monitoreo y revisión de informes de gestión o reportes
	Seguimiento a indicadores de gestión por procesos, planes, programas, proyectos
	Monitoreo y revisión de riesgos
	Seguimiento a bases de datos
	Seguimiento a instrumentos de planificación de largo, mediano y corto plazo
	Validación de información por parte de un sistema o aplicativo
OPERATIVOS	Aplicación de listas de chequeo, formatos estandarizados
	Capacitación/ divulgación/ socialización
	Validación de información por parte de una persona o comité (revisión, comparación, verificación, validación, inspección, conciliación)
	Copias de seguridad, contingencias y respaldo de información, planes de continuidad del negocio
	Custodia apropiada de la información
	Seguros o pólizas
	Realización de visitas en sitio
	Segregación de funciones
LEGALES	Actualización de normatividad
	Seguimiento al cumplimiento de normas o tiempos de respuesta

Fuente: Corpocaldas, Elaboración propia, 2024.

Las desviaciones calificadas como recurrentes serán informadas por parte de la Oficina de Control interno y/o el subproceso de mejora continua, al comité de coordinación de control interno, para gestionar los correctivos necesarios a través de la primera y segunda línea.

La evaluación se realizará de acuerdo a la periodicidad de cada uno de los controles, si la desviación supera el **50%** se calificará como **recurrente** y se llevará a cabo el procedimiento anterior.

15. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

En el evento de materializarse un riesgo se procederá de la siguiente forma:

Tabla 11. Descripción de acciones y responsables ante riesgos materializados

TIPO DE RIESGO	RESPONSABLE	ACCIÓN
Riesgo de Corrupción y fiscal	Líder de Proceso Oficina de Control Interno	• Informar a la línea estratégica sobre el posible hecho encontrado para determinar el proceso a seguir de conformidad con la ley aplicable. • Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. • Revisar los controles existentes y actualizar el mapa de riesgos cuando se considere pertinente.
Riesgos de Gestión y Seguridad de la información	Líder de Proceso	• Realizar los correctivos necesarios e iniciar el análisis de causas y determinar acciones correctivas, preventivas y de mejora, así como la revisión de los controles existentes, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos cuando se considere pertinente. • Dar cumplimiento al Procedimiento de implementación de acciones preventivas y correctivas.
	Oficina de Control Interno	• Informar al líder del proceso sobre el hecho encontrado. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos si se considera pertinente. • Si la materialización de los riesgos se evidencia en una auditoría interna o externa, la OCI verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.

Fuente: Corpocaldas, Elaboración propia, diciembre de 2021.

16. DIVULGACION

La Política de Administración del Riesgo y los Mapas de Riesgos de Gestión, Corrupción, Fiscales y Seguridad de la Información se divulgarán a través de comunicación internas y en el aplicativo del sistema de gestión integrado, a fin de que todas las partes interesadas estén enteradas de manera permanente de los riesgos identificados por la entidad para proceder con la gestión de los mismos. El mapa de riesgos de corrupción se publicar en la página web de la Corporación Autónoma Regional.

17. CAPACITACION

La administración del riesgo se considera un tema importante para la entidad, por ello se realiza como mínimo una capacitación anual (interna), que permita fortalecer las competencias de los servidores públicos, y así poder garantizar una gestión del riesgo coherente y adecuada, dentro de cada uno de los procesos.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
01	Diciembre 23 de 2021	Versión inicial del documento. Resolución 212-2335 del 2021
O2	Diciembre 30 de 2025	La política se actualizó en los siguientes aspectos: 1. Articulación y actualización con los lineamientos de la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 06, 2022 en cuanto a los lineamientos para el análisis de riesgo fiscal. 2. Se actualizo las estrategias de seguimiento y monitoreo de acuerdo con los periodos y frecuencias establecidos dadas las dinámicas de la Corporación. 3. Se actualiza el Modelo de las tres líneas de defensa, roles y responsabilidades en Corpocaldas