CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR
-CORPOCESAR-

RESOLUCIÓN No. 0368 14 JUL 2026

"POR MEDIO DE LA CUAL SE ACTUALIZA Y ADOPTA LA POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR, Y SE DICTAN OTRAS DISPOSICIONES."

La Directora General de la Corporación Autónoma Regional del Cesar – CORPOCESAR, en ejercicio de las facultades legales y estatutarias, en especial las conferidas por la Ley 99 de 1993, el Decreto 1083 de 2015, el Decreto 648 de 2017, el Decreto 1499 de 2017, el Decreto 1662 de 2021 y demás normas concordantes,

CONSIDERANDO:

Que el artículo 269 de la Constitución Política de 1991 establece que las entidades públicas, están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de Control Interno, de conformidad con lo que dispone la Ley;

Que literal a) del artículo 2° de la Ley 87 del 29 de noviembre de 1993 "Por la cual se establecen normas para el ejercicio de Control Interno en las entidades y organismos del Estado y se dictan otras disposiciones", establece que se deben proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten;

Que la Ley 489 del 29 de diciembre de 1998 "Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones", en su artículo 28, referente al fortalecimiento del Sistema de Control Interno de las instituciones públicas, dispuso la aplicación de instrumentos de gerencia, con el fin de fortalecer el cumplimiento cabal y oportuno de las funciones del Estado;

Que el artículo 4º del Decreto 648 del 19 de abril de 2017, adiciona en el Capítulo 1 del Título 21 del Decreto 1083 del 26 de mayo de 2015, el artículo 2.2.21.1.6 relacionado con las funciones del Comité Institucional de Coordinación de Control Interno, incorporando como una de las funciones de este Comité la que debe 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.

Que el artículo 8º del Decreto 648 del 19 de abril de 2017 modificó el artículo 2.2.21.3.1 del Decreto 1083 del 26 de mayo de 2015, estableciendo que el Sistema Institucional de Control Interno estará integrado por el esquema de controles de la organización, la gestión de riesgos, la administración de la información y de los recursos y por el conjunto de planes, métodos, principios, normas, procedimientos, y mecanismos de verificación y evaluación adoptados por la entidad, dentro de las políticas trazadas por la dirección y en atención a las metas, resultados u objetivos de la entidad."

Que el artículo 17º del Decreto 648 del 19 de abril de 2017, modifica el artículo 2.2.21.5.3 del Decreto 1083 del 26 de mayo de 2015, relacionado con las oficinas de control interno, estableciendo que las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control.

Que el artículo 2.2.21.5.4 del Decreto 1083 del 26 de mayo de 2015, relacionado con la Administración de riesgos, establece que como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces,

evaluando los aspecto tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.

Que el artículo 2.2.21.5.5 del Decreto 1083 del 26 de mayo de 2015, relacionado con las políticas de control interno diseñadas por el Departamento Administrativo de la Función Pública, establece que las guías, circulares, instructivos y demás documentos técnicos elaborados por el Departamento Administrativo de la Función Pública, constituirán directrices generales a través de las cuales se diseñan las políticas en materia de control interno, las cuales deberán ser implementadas al interior de cada organismo y entidad del Estado. Así mismo, precisa que el Departamento Administrativo de la Función Pública elaborará prioritariamente guías e instructivos sobre elaboración de manuales de procedimientos, y sobre diseño de indicadores para evaluar la gestión institucional, los cuales se constituirán en herramientas básicas de eficiencia y transparencia de las organizaciones.

Que el artículo 73 de la Ley 1474 del 12 de julio de 2011 determina que cada entidad del orden nacional deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano, la cual debe contemplar, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad y las medidas concretas para mitigar esos riesgos, en concordancia con lo establecido en la política de transparencia, participación y servicio al ciudadano, componente plan anticorrupción del nuevo modelo integrado de planeación y gestión, recientemente reglamentado mediante el Decreto 1499 del 11 de septiembre de 2017.

Que la Dimensión 7 del Modelo Integrado de Planeación y Gestión - MIPG, denominada Direccionamiento Estratégico y Planeación, establece en su Política de Planeación Institucional, que una de las acciones de implementación de dicha política, consiste en que se deben atender las recomendaciones para formular los lineamientos para administración del riesgo, es decir, la Política de Riesgo, como una tarea propia del equipo directivo y se debe hacer desde el ejercicio de Direccionamiento Estratégico y de Planeación.

Que la gestión integral del riesgo constituye una herramienta estratégica para fortalecer la gobernanza institucional, la toma de decisiones, la prevención de eventos que puedan afectar el cumplimiento de la misión institucional y la generación de valor público, mediante la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos asociados a los procesos de la Corporación.

Que en el marco de la modernización del Estado Colombiano y la implementación de un enfoque basado en resultados, la gestión de riesgos se consolida como una herramienta fundamental para fortalecer la toma de decisiones públicas, la transparencia, la eficacia institucional y la confianza ciudadana. Más allá de su función preventiva, la gestión de riesgos permite anticipar escenarios adversos, gestionar oportunidades y alinear la operación institucional con los objetivos estratégicos del Estado.

Que por medio de la Resolución 0141 del 9 de abril del 2021 se actualiza y reglamenta la Política de Administración de Riesgos y Diseño de Controles en la CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR, con base en lo establecido tanto en el Modelo Integrado de Planeación y Gestión MIPG, como en el Sistema de Control Interno SCI y en la Guía para la Administración del Riesgo y el Diseño de Controles, Versión 5, de Diciembre de 2020, expedida por el Departamento Administrativo de la Función Pública – DAFP, y se dictan otras disposiciones.

Que de acuerdo a lo establecido en la Guía para la Gestión Integral del Riesgo Versión 7 emitida por el Departamento Administrativo de la Función Pública – DAFP, se hace necesario establecer, documentar, aplicar y adoptar la Metodología y los Instrumentos Técnicos necesarios para la Gestión

Continuación Resolución No. 0368 de 14 JUL 2026 "POR MEDIO DE LA CUAL SE ACTUALIZA Y ADOPTA LA POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR, Y SE DICTAN OTRAS DISPOSICIONES." ---------- 3

Integral del Riesgo en la CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR, en la que se mantenga la estructura conceptual y metodológica general para la gestión del riesgo bajo un enfoque integral, atendiendo las políticas de gestión y desempeño que se vinculan y su relación con otras políticas; que se tratará la gestión integral del riesgo, con elementos comunes aplicables a todas las tipologías de riesgo, incluyendo contenidos del marco COSO-ERM (2017) que precisan y profundizan los conceptos de riesgo, gestión del riesgo y niveles de madurez del riesgo; que se precisan contenidos conceptuales relacionados con la gestión preventiva de riesgos fiscales, riesgos asociados a posibles actos de corrupción, de acuerdo con el componente programático denominado Estrategia Institucional para la Lucha Contra la Corrupción y el Programa de Transparencia y Ética Pública de la Corporación, y los riesgos de seguridad de la información.

Que, conforme a lo anterior, se hace necesario actualizar y adoptar la Política para la Gestión Integral del Riesgo de la Corporación Autónoma Regional del Cesar – CORPOCESAR, con el fin de fortalecer la gestión institucional, el Sistema de Control Interno y la cultura de gestión del riesgo, en armonía con los lineamientos establecidos por el Departamento Administrativo de la Función Pública – DAFP.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO. Actualización y adopción de la Política para la Gestión Integral del Riesgo. Actualizar y adoptar la Política para la Gestión Integral del Riesgo de la Corporación Autónoma Regional del Cesar – CORPOCESAR, la cual hace parte integral de la presente Resolución y será de obligatorio cumplimiento para todos los servidores públicos, contratistas y demás colaboradores que desarrollen actividades en nombre de la Corporación, en el marco de sus competencias y responsabilidades.

ARTÍCULO SEGUNDO. Finalidad. La actualización de la Política para la Gestión Integral del Riesgo de la Corporación Autónoma Regional del Cesar – CORPOCESAR tiene como finalidad armonizar su contenido con los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, expedida por el Departamento Administrativo de la Función Pública – DAFP, con el propósito de fortalecer la gestión institucional, el Sistema de Control Interno y la cultura de gestión del riesgo, mediante la identificación, análisis, valoración, tratamiento, comunicación, monitoreo y seguimiento de las diferentes tipologías de riesgo que puedan afectar el cumplimiento de la misión institucional, los objetivos estratégicos, los procesos, los proyectos, la prestación de los servicios y la generación de valor público.

La Política será de aplicación obligatoria en todos los procesos de la Corporación y orientará la gestión de las diferentes tipologías de riesgo aplicables a la Entidad, promoviendo la toma de decisiones basada en riesgos, el fortalecimiento del Sistema de Control Interno, la mejora continua y el cumplimiento de la normatividad vigente.

ARTICULO TERCERO. Responsabilidades de los servidores públicos y demás colaboradores. Los servidores públicos y demás colaboradores de CORPOCESAR, en el ámbito de sus competencias y responsabilidades, deberán conocer, aplicar y cumplir las disposiciones contenidas en la Política de Gestión Integral del Riesgo, contribuyendo a su implementación, mantenimiento y mejora continua. En desarrollo de lo anterior, les corresponde:

a) Identificar, analizar, valorar, tratar, monitorear y reportar oportunamente los riesgos asociados a los procesos, actividades, proyectos y demás asuntos bajo su responsabilidad, de conformidad con la metodología institucional vigente.

b) Implementar y mantener los controles y acciones de tratamiento definidos en los Mapas de Riesgos, garantizando su ejecución, seguimiento y actualización cuando las condiciones internas o externas así lo requieran.

c) Reportar de manera oportuna al líder del proceso las situaciones que puedan generar nuevos riesgos, la materialización de riesgos existentes, las debilidades en los controles o cualquier circunstancia que pueda afectar el logro de los objetivos institucionales.

d) Participar en las actividades de capacitación, sensibilización y fortalecimiento de la cultura de gestión del riesgo que promueva la Corporación.

e) Suministrar información veraz, completa y oportuna para el seguimiento, evaluación y mejora de la Gestión Integral del Riesgo.

f) Contribuir al fortalecimiento de una cultura organizacional basada en la prevención, el autocontrol, la autorregulación, la transparencia, la mejora continua y la adecuada gestión de los riesgos, en concordancia con los lineamientos institucionales y la normatividad vigente.

g) Informar inmediatamente al líder del proceso y a las instancias competentes la materialización de riesgos, incidentes o eventos que puedan afectar el cumplimiento de los objetivos institucionales, con el fin de adoptar oportunamente las medidas de respuesta correspondientes.

NIVELES DE AUTORIDAD Y RESPONSABILIDADES – ROLES

LINEA ESTRATÉGICA - ALTA DIRECCIÓN - Y COMITÉ DE COORDINACIÓN DE CONTROL INTERNO	Define y aprueba la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2a línea identificadas, con base en lo cual toma acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad y teniendo en cuenta el enfoque preventivo.
PRIMERA LINEA DE DEFENSA – LÍDERES DE PROCESOS Y EQUIPOS DE TRABAJO	Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de controles, por lo que se trata de definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados, alineados con las metas y objetivos de la Corporación y proponer mejoras a la gestión del riesgo en su proceso y reportar a la segunda y tercera línea de defensa (Subdirección de Planeación y Oficina de Control Interno) los avances y evidencias de la gestión del riesgo en los plazos establecidos.
SEGUNDA LINEA DE DEFENSA-SUBDIRECCIÓN GENERAL ÁREA DE PLANEACIÓN	Corresponde al seguimiento periódico de todos los riesgos por la Oficina de Planeación, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de primera línea puedan establecer mejoras a los controles y a los riesgos, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los lideres de los procesos y sus equipos para la mejora de ese tema.

TERCERA LINEA DE DEFENSA - JEFE OFICINA DE CONTROL INTERNO	Seguimiento y evaluación a través de la auditoría interna para verificar y establecer la efectividad de los controles para evitar la materialización de riesgos. El funcionario Responsable y líder del proceso de Control Interno evalúa de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la 2ª línea de defensa. A través del Plan Anual de Auditorias propone esquemas de asesoría y acompañamiento a la entidad, actividades que pueden coordinar con la Subdirección de Planeación; monitore a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo; Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos; formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos; Informar los hallazgos y proporcionar recomendaciones de forma independiente; Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos; proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa; recomendar mejoras a la política de operación para la administración del riesgo; e Informar sobre las auditorías basadas en riesgos que se ejecuten, con énfasis en riesgos fiscales.

Fuente: Departamento Administrativo de la Función Pública – DAFP. Guía para la Gestión Integral del Riesgo en Entidades Públicas. Versión 7. 2025.

El incumplimiento de las responsabilidades previstas en el presente artículo dará lugar a las actuaciones administrativas, disciplinarias o de otra índole a que haya lugar, de conformidad con la Constitución Política, la ley y las normas internas aplicables.

ARTÍCULO CUARTO. Instrumentos para la Gestión Integral del Riesgo. Hacen parte integral de la presente Resolución la Política para la Gestión Integral del Riesgo, las matrices de mapas de riesgos y los demás documentos, metodologías, procedimientos, instructivos, formatos e instrumentos técnicos que se adopten para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos, en el marco del Sistema Integrado de Gestión de la Corporación.

Los documentos e instrumentos a que se refiere el presente artículo serán de aplicación obligatoria en todos los procesos de CORPOCESAR y podrán ser actualizados, ajustados o complementados cuando las necesidades institucionales, los cambios normativos, las metodologías vigentes o las características propias de los procesos y de las diferentes tipologías de riesgo así lo requieran, siempre que dichas modificaciones sean aprobadas por la instancia competente, de conformidad con los lineamientos institucionales para la Gestión Integral del Riesgo, sin que ello implique la modificación de la presente Resolución.

ARTÍCULO QUINTO. Comunicación. Comunicar la presente Resolución a todas las dependencias de la Corporación Autónoma Regional del Cesar – CORPOCESAR, para su conocimiento, implementación

Continuación Resolución No. 0368 de 14 JUL 2026 "POR MEDIO DE LA CUAL SE ACTUALIZA Y ADOPTA LA POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL CESAR – CORPOCESAR, Y SE DICTAN OTRAS DISPOSICIONES." ---------- 6

y estricto cumplimiento, así como disponer su publicación en los medios institucionales correspondientes, de conformidad con la normatividad vigente.

ARTÍCULO SEXTO: La presente Resolución rige a partir de la fecha de su expedición y deroga la Resolución 0141 del 9 de abril del 2021.

Dado a los,

14 JUL 2026

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

ADRIANA MARGARITA GARCIA ARÉVALO
Directora General

	Nombre Completo	Firma
Proyectó	Ing. Hanne Sánchez M. / Profesional de Apoyo SGAP - SIGC	
Revisó	María Cristina Robayo Abello / Subdirectora General de Planeación	
Aprobó	Almes José Granados Cuello / Asesor de Dirección	
Los arriba firmantes declaramos que hemos revisado el documento con sus respectivos soportes y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para su firma.		

INTRODUCCIÓN

En un entorno caracterizado por rápidos cambios, complejidad operativa y exigencias de transparencia y eficiencia, la gestión adecuada de los riesgos constituye un elemento esencial para garantizar la sostenibilidad, cumplimiento y creación de valor institucional. CORPOCESAR, comprometida con sus principios de integridad, responsabilidad y mejora continua, adopta la presente **Política de Administración de Riesgos** como marco rector para fortalecer su cultura organizacional y orientar la identificación, evaluación, tratamiento, seguimiento y control de los riesgos que puedan impactar el logro de sus objetivos estratégicos y operativos.

La administración del riesgo en la Corporación Autónoma Regional del Cesar - CORPOCESAR se desarrolla en coherencia con el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno – MECI, las disposiciones del Decreto 1499 de 2017, y se enmarca y actualiza conforme a los lineamientos establecidos en la **Guía de Administración de Riesgos DAPF Versión 7** del Departamento Administrativo de la Función Pública, reflejando las mejores prácticas internacionales y los requisitos normativos aplicables al sector público colombiano. Este enfoque permite integrar la gestión de riesgos dentro de los procesos institucionales, promueve la toma de decisiones informada y proactiva, y fortalece la resiliencia ante incertidumbres internas y externas.

CORPOCESAR reconoce que la administración de riesgos es responsabilidad de todos los servidores públicos y partes interesadas, y que su adecuada implementación contribuye a la protección de los recursos públicos, el cumplimiento de la misión institucional, la confianza de los ciudadanos y la consecución de los fines públicos con eficiencia, eficacia y ética.

Esta política aplica a todos los procesos, proyectos, productos y actividades desarrollados por las áreas y servidores de la entidad, quienes deben incorporar la administración del riesgo en el ejercicio de sus funciones y en la planeación de su gestión.

La Política de Administración del Riesgo recoge la estrategia definida por la Alta Dirección, enfocada en la identificación, análisis, tratamiento y monitoreo de los riesgos de gestión, corrupción, fraude, fiscales, de seguridad de la información y de daño antijurídico, promoviendo el diseño e implementación de controles que mitiguen la

probabilidad de ocurrencia y el impacto de eventos adversos. Así mismo, orienta la preparación y ejecución de acciones de contingencia ante la materialización de dichos riesgos, garantizando la continuidad institucional, la sostenibilidad operativa y la protección del interés público.

Para la Corporación Autónoma Regional del Cesar – CORPOCESAR, la política de gestión integral de riesgos debe considerar los principios de:

Responsabilidad compartida: La gestión del riesgo es responsabilidad de todos los servidores públicos.

Enfoque estratégico: Los riesgos se gestionan en función del cumplimiento del Plan de Acción Institucional y los objetivos estratégicos.

Transparencia y trazabilidad: Las decisiones frente a riesgos deben ser documentadas y verificables.

Mejora continua: La gestión de riesgos se revisa y ajusta periódicamente.

Enfoque preventivo: Prioriza la anticipación sobre la reacción.

MARCO NORMATIVO

Anticorrupción Artículo 73. "Plan Anticorrupción y de Atención al Ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.

Decreto 1649 de 2014 Funciones de la Secretaría de Transparencia: 13) Señalar la metodología para diseñar y hacer seguimiento a las estrategias de lucha contra la corrupción y de atención al ciudadano que deberán elaborar anualmente las entidades del orden nacional y territorial.

ISO 9001: Norma Técnica Colombiana, elaborada por la Organización Internacional para la Estandarización (International Standarization Organization o ISO por sus siglas en inglés), determina los requisitos para un Sistema de Gestión de la Calidad.

Decreto 1081 de 2015: Señala como metodología para elaborarla estrategia de lucha contra la corrupción la contenida en el documento "Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.

Decreto Nacional 1499 de 2017: hace necesario adoptar para la Alcaldía municipal el MIPG, como el nuevo marco de referencia para el diseño e implementación del SIG, con el fin de fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades de la alcaldía municipal adecuar la institucionalidad del sistema y de las instancias correspondientes con el modelo nacional.

ISO 31000:2018: Norma Técnica Internacional Administración del Riesgo- Principios y orientaciones.

DAFP - Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 Agosto de 2025.

OBJETIVOS

OBJETIVO GENERAL

Establecer el marco institucional para la adecuada administración de los riesgos en CORPOCESAR, mediante la definición de lineamientos, responsabilidades y metodologías que permitan identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos que puedan afectar el cumplimiento de la misión, los objetivos estratégicos, los procesos institucionales y la adecuada gestión de los recursos públicos.

OBJETIVOS ESPECIFICOS

- ✓ Orientar la toma de decisiones bajo un enfoque preventivo y basado en riesgos, definiendo el apetito de riesgo institucional como el nivel de riesgo que la entidad está dispuesta a aceptar en el desarrollo de sus funciones, y estableciendo criterios claros para el tratamiento y escalamiento de riesgos que superen los niveles tolerables.

- ✓ Fortalecer la cultura de gestión del riesgo integrado a la planeación institucional, promoviendo la toma de decisiones informada, el autocontrol, la transparencia, la integridad y la mejora continua.

- ✓ Adoptar el esquema de líneas de defensa como modelo de gobernanza, delimitando responsabilidades entre la gestión operativa (primera línea), la supervisión y acompañamiento (segunda línea) y la evaluación independiente (tercera línea), con el propósito de fortalecer el autocontrol, la transparencia, la eficiencia administrativa y la protección de los recursos públicos.

ALCANCE

La Política de Administración de Riesgos aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación de CORPOCESAR, y compromete a todos los servidores públicos, directivos, contratistas y demás actores que participen en la gestión institucional.

Comprende la administración integral de los riesgos estratégicos, operativos, financieros, de cumplimiento, de corrupción, de fraude, de daño antijurídico, tecnológicos y seguridad de la información, y ambientales, incorporando su análisis dentro de la planeación institucional, la formulación de proyectos, la gestión contractual y la toma de decisiones directivas.

La política opera bajo el modelo de líneas de defensa, en el cual la primera línea gestiona y controla los riesgos en los procesos; la segunda línea orienta, consolida y supervisa la gestión del riesgo; la tercera línea evalúa de manera independiente la efectividad del sistema.

DEFINICIONES

Administración de riesgos: 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (INTOSAI, 2000).

Análisis de riesgo: Uso sistemático de la información disponible para valorar los riesgos en función de las causas o agentes que los generan, las consecuencias generadas por un incidente y/o evento, su severidad y la posibilidad de ocurrencia del mismo, con el fin de estimar la zona de riesgo inicial (riesgo inherente).

Apetito de riesgo: es el nivel de riesgo que una entidad está dispuesta a asumir 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 gestionar.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad. (relacionado con la solvencia y liquidez).

Causa: Medios, circunstancias, situaciones o agentes generadores del riesgo. Algunas fuentes de riesgos son: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Consecuencia: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento

Control: Cualquier medida que adopte la entidad para gestionar los riesgos y proporcionar una seguridad razonable de alcanzar los objetivos y metas establecidos

Evaluación del riesgo: Determinación de las prioridades de gestión del riesgo, mediante la comparación del nivel de riesgo hallado (riesgo inherente) y la evaluación de las medidas de control existentes. Es una etapa que busca confrontar los resultados del análisis de riesgo

inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).

Gestión del riesgo: Es el conjunto de "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Contempla las etapas de política de administración del riesgo, construcción del mapa de riesgos, comunicación y consulta, monitoreo y revisión y seguimiento.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
Nota 1: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

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

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

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

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Programa de Transparencia y Ética Pública (PTEP): es una estrategia obligatoria para entidades públicas en Colombia, creada por la Ley 2195 de 2022, que busca prevenir la corrupción, promover la cultura de la legalidad, gestionar riesgos, mejorar el acceso a la información y servicios, y fomentar la participación ciudadana y rendición de cuentas.

CICCI: Comité Institucional de Coordinación de Control Interno.

CGDI: Comité de Gestión y Desempeño Institucional. Fraude: Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Mapas de riesgo: Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.

MIPG: Modelo Integrado de Planeación y Gestión.

MECI: Modelo Estándar de Control Interno Restablecimiento: Capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.

Riesgos Operativos: Posibilidad de incurrir en pérdidas por errores, fallas o deficiencias en el Talento Humano, Procesos, Tecnología. Infraestructura y Eventos Externos.

Riesgo inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riego inherente, dentro de unas escalas de severidad.

Riesgo residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Tolerancia del 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.

Tratamiento del riesgo: Proceso para modificar el riesgo.

Valoración del Riesgo: Establece la identificación y evaluación de los controles. En la etapa de valoración del riesgo se determina el riesgo residual.

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

METODOLOGÍA APLICADA

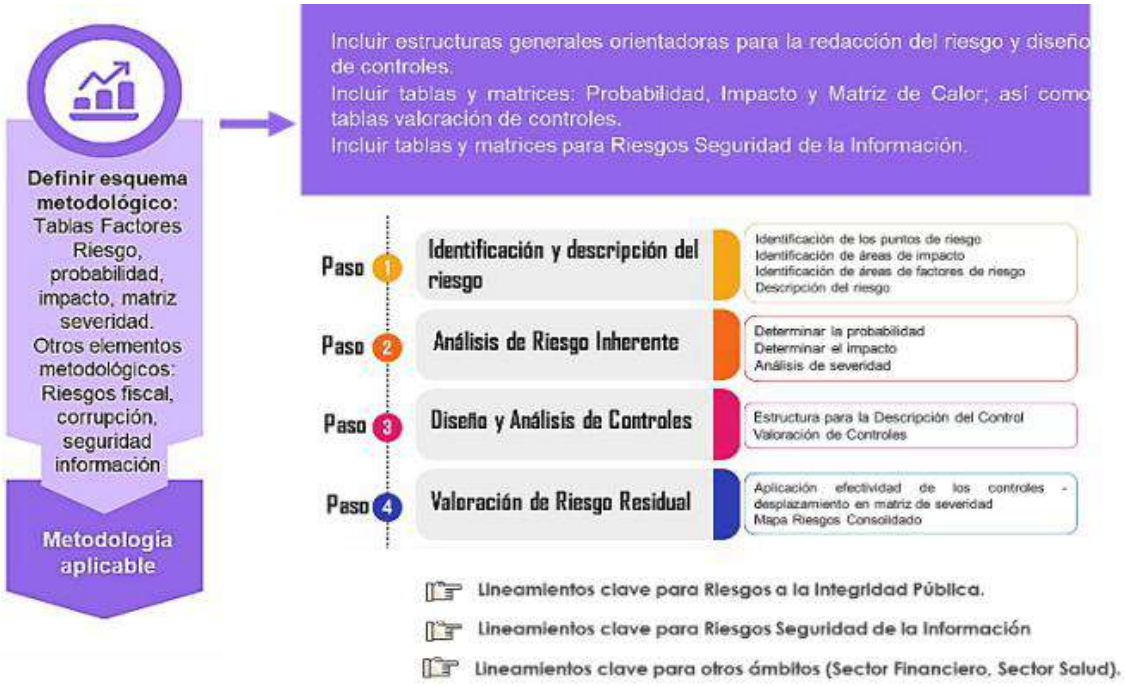
La presente Política de Administración del Riesgo desarrolla su gestión siguiendo los lineamientos fundamentales establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas– Versión 7 (2025), emitida por el Departamento Administrativo de la Función Pública – DAFP, asegurando su coherencia con el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno – MECI, y la Norma ISO 31000:2018.

La gestión integral de riesgos, es posible definirla como “la cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo, de cara a la creación, preservación y materialización de valor.” (IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.10). Esta definición, adoptada, implica que la gestión del riesgo se consolida a través de: i) el reconocimiento de la cultura; ii) el desarrollo de capacidades; iii) el uso de las técnicas aplicadas; iv) la integración de la estrategia y el desempeño; v) la alineación con la estrategia y objetivos clave y vi) la relación con el valor.

La metodología aplicada se estructura en tres (3) pasos estratégicos fundamentales, que permiten la identificación, análisis del riesgo inherente, diseño y análisis de controles de los riesgos y valoración del riesgo residual de manera sistemática, garantizando la integración de la gestión de riesgos en todos los procesos, planes, proyectos y actividades de la Corporación Autónoma Regional del Cesar - CORPOCESAR.

Para su implementación efectiva la política será necesario desplegar una estructura metodológica tomando como referencia la dispuesta en la guía, considerando elementos básicos como i) tabla factores de riesgo; ii) tablas de probabilidad e impacto; iii) matriz de severidad; iv) tabla valoración controles. Así mismo, se incluye lineamientos clave para los riesgos a la Integridad Pública, riesgos fiscales y riesgos de seguridad de información, así como otros marcos y normatividad aplicable.

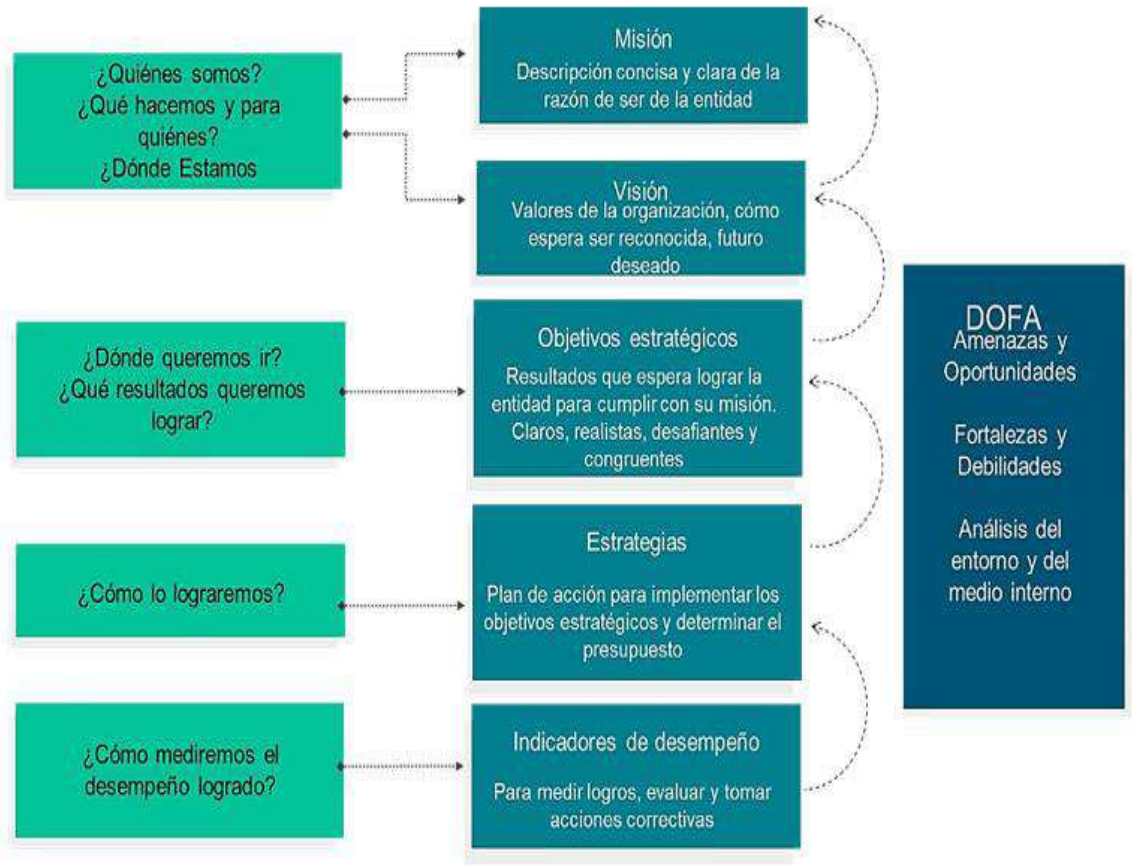
A continuación, se presenta la estructura operativa de la metodología, con sus desarrollos básicos, que sirven como guía para la aplicación coherente y sistemática de la política en toda la Corporación:



ANÁLISIS ESTRATÉGICO DE LA ENTIDAD Y SU MODELO DE OPERACIÓN BASADA EN PROCESOS:

Para el análisis estratégico de la entidad es necesario que el Modelo Integrado de Planeación y Gestión (MIPG) sea visto de manera integral, dado que las políticas y dimensiones que lo integran se articulan de manera directa con una adecuada gestión por procesos. En particular, la dimensión de Direccionamiento Estratégico contempla que una entidad debe realizar un análisis del entorno tanto específico como general, así como un análisis de capacidades internas. Se desarrolla un modelo básico de planeación estratégica, donde se precisan las preguntas que pueden orientar la construcción de cada uno de los componentes

Figura 4 Modelo básico de planeación estratégica



Niveles de Madurez para la Gestión del Riesgo:

Teniendo en cuenta que la gestión estratégica del riesgo involucra una serie de componentes y elementos que se deben fortalecer desde la cultura organizacional, se hace necesario evaluar su nivel de madurez. Para este efecto, atendiendo uno de los marcos que sustentan el desarrollo de la Guía se propone una estructura que, "*consta de cinco componentes interrelacionados de la gestión del riesgo empresarial y su relación con la misión, visión y valores clave de la entidad*". Gráficamente se observan "*tres cintas que muestran el Establecimiento de Estrategias y de los Objetivos, Desempeño, Revisión y Monitorización representan los procesos más habituales que fluyen a través de la entidad. Las otras dos cintas de, Gobierno y cultura, e Información, Comunicación y Reporte, representan aspectos de apoyo a la gestión del riesgo empresarial*". Así, en una gestión integral del riesgo, la aplicación y el desarrollo de estas políticas implican:

Fuente: IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017

Los cinco componentes que integran una óptima gestión del riesgo a la luz de este marco de referencia se describen a continuación:

Gobierno y Cultura: El gobierno y cultura juntos forman una base para todos los demás componentes de la gestión del riesgo empresarial. El gobierno marca el tono de la entidad, reforzando la importancia de la gestión del riesgo institucional y estableciendo responsabilidades de supervisión al respecto. La cultura se refleja en la toma de decisiones.

Establecimiento de la estrategia y objetivos: La gestión del riesgo empresarial se integra en el plan estratégico de la entidad a través del proceso de establecimiento de la estrategia y de los objetivos institucionales. Con un conocimiento profundo del contexto institucional, la organización puede comprender mejor los factores internos y externos y sus efectos en el riesgo.

Desempeño: Una organización identifica y evalúa los riesgos que pueden afectar la capacidad de una entidad para alcanzar la estrategia y los objetivos institucionales. La organización entonces selecciona las respuestas al riesgo y efectúa seguimiento del desempeño considerando posibles cambios.

Revisión y monitorización: Al examinar las capacidades y técnicas de gestión del riesgo institucional, y el desempeño de la entidad en relación con sus objetivos.

Información, Comunicación y Reporte: La comunicación es el proceso continuo e iterativo de obtener y compartir información en toda la entidad. La Dirección utiliza información pertinente de fuentes internas y externas para facilitar la gestión del riesgo institucional. La organización aprovecha los sistemas de información para capturar, procesar y gestionar datos e información. Al utilizar información que se aplica a todos los componentes, la organización informa sobre el riesgo, la cultura y el desempeño. (IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.11, 12).

CONTEXTO INTERNO Y EXTERNO

Para garantizar una gestión integral del riesgo alineada con los objetivos institucionales, es necesario desplegar un análisis interno y externo específico para la entidad, donde se expliquen mediante información institucional formalizada y datos específicos relacionados, teniendo en cuenta los siguientes elementos:

✓ **Contexto Interno**: estructura organizacional, cultura institucional, capacidad tecnológica, talento humano, procesos internos, recursos financieros, políticas internas y marco normativo aplicable.

✓ **Contexto Externo**: entorno político, económico, social, ambiental y tecnológico; actores del sector, reguladores, organismos de control, ciudadanos y partes interesadas, así como riesgos asociados a cambios normativos y eventos externos. Sector donde opera la entidad y su relacionamiento con otras entidades e instancias necesarias para su gestión, así como entorno de desarrollo territorial.

El análisis del contexto permite identificar aquellos riesgos que podrían afectar el cumplimiento de los objetivos estratégicos, asegurando que la gestión del riesgo se enfoque en los eventos con mayor impacto institucional

CONTEXTO ESTRATEGICO	
CONTEXTO EXTERNO	**Económicos**: Disponibilidad de Capital, Liquidez; mercados financieros, desempleo, competencia.
	Políticos: Cambio de Gobiernos, Legislación, Políticas Públicas, regulación.
	Sociales y Culturales: Demografía, responsabilidad social, Orden Público.
	T**ecnológico**: Avances en tecnologías, Accesos a sistema de información externo, Tecnología emergente, Gobierno en Línea.
	Medioambientales: Condiciones ambientales, emisiones, residuos, energía, agua, catástrofes naturales, desarrollo sostenible,
	Comunicación Externa: Mecanismos para estar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.
CONTEXTO INTERNO	**Financieros**: Presupuesto de funcionamiento, recurso de inversión, infraestructura, capacidad instalada.
	Personal: Evaluar la Competencia del personal, Identificar oportunidades de desarrollo profesional, disponibilidad.
	Proceso: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento
	Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información
	Estructura Organizacional: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.

	Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones
CONTEXTO DEL PROCESO	**Diseño de Procesos**: Claridad en la descripción, alcance, objetivos del proceso
	Interacción con otros Procesos: Relación precisa con otros procesos en cuanto al insumo, proveedores, producto, usuario cliente.
	Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	Procedimientos Asociados: Pertinencia en los procedimientos que desarrollan los procesos.
	Responsables del Proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación Entre Procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.

NIVELES DE AUTORIDAD Y RESPONSABILIDADES – ROLES

LINEA ESTRATÉGICA - ALTA DIRECCIÓN - Y COMITÉ DE COORDINACIÓN DE CONTROL INTERNO	Define y aprueba la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2a línea identificadas, con base en lo cual toma acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad y teniendo en cuenta el enfoque preventivo.
PRIMERA LINEA DE DEFENSA – LÍDERES DE PROCESOS Y EQUIPOS DE TRABAJO	Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de controles, por lo que se trata de definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados, alineados con las metas y objetivos de la Corporación y proponer mejoras a la gestión del riesgo en su proceso y reportar a la segunda y tercera línea de defensa (Subdirección de Planeación y Oficina de Control Interno) los avances y evidencias de la gestión del riesgo en los plazos establecidos.
SEGUNDA LINEA DE DEFENSA- SUBDIRECCIÓN GENERAL ÁREA DE PLANEACIÓN	Corresponde al seguimiento periódico de todos los riesgos por la Oficina de Planeación, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de primera línea puedan establecer mejoras a los controles y a los riesgos, así mismo garantizar su aplicación efectiva, lo que implica que se deben

	incorporar ejercicios de asesoría y acompañamiento a los lideres de los procesos y sus equipos para la mejora de ese tema.
TERCERA LINEA DE DEFENSA -JEFE OFICINA DE CONTROL INTERNO	Seguimiento y evaluación a través de la auditoría interna para verificar y establecer la efectividad de los controles para evitar la materialización de riesgos. El funcionario Responsable y líder del proceso de Control Interno evalúa de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la 2ª línea de defensa. A través del Plan Anual de Auditorias propone esquemas de asesoría y acompañamiento a la entidad, actividades que pueden coordinar con la Subdirección de Planeación; monitore a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo; Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos; formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos; Informar los hallazgos y proporcionar recomendaciones de forma independiente; Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos; proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa; recomendar mejoras a la política de operación para la administración del riesgo; e Informar sobre las auditorías basadas en riesgos que se ejecuten, con énfasis en riesgos fiscales.

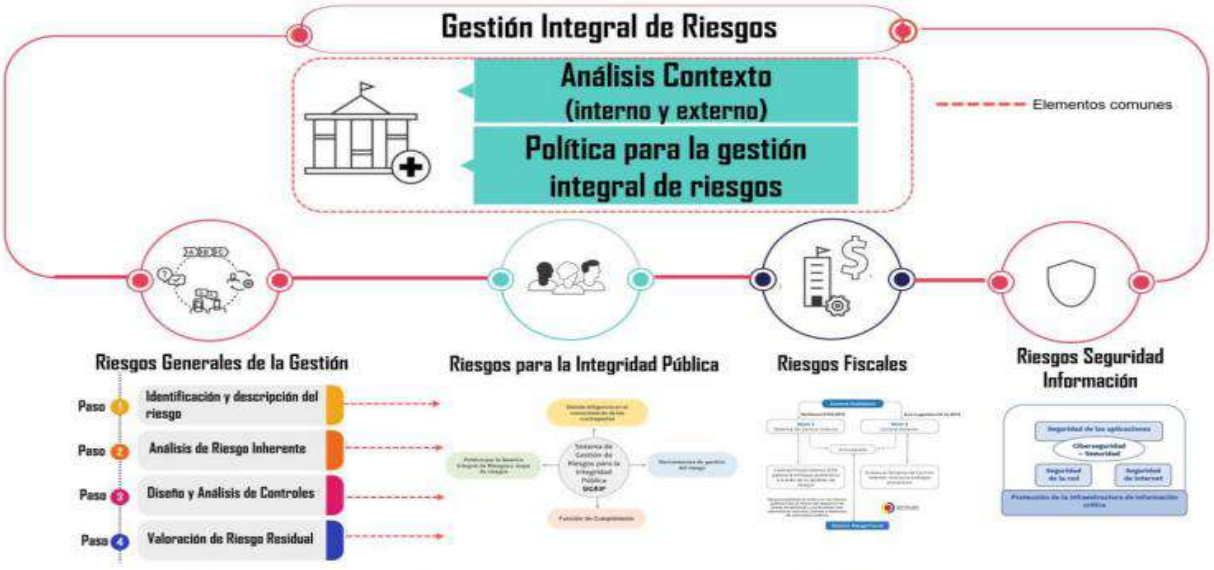
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Publicad Versión 7 de 2025

ESQUEMA METODOLÓGICO APLICABLE

Para que la Corporación Autónoma Regional del Cesar – CORPOCESAR, desarrolle la Política de Administración de Riesgos, se hace necesario desplegar una estructura metodológica tomando como referencia los lineamientos establecidos por el **Departamento Administrativo de la Función Pública (DAFP) en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025)**, considerando elementos básicos como i) tabla factores de riesgo; ii) tablas de probabilidad e impacto; iii) matriz de severidad; iv) tabla valoración controles. Así mismo, incluir lineamientos clave para los riesgos a la Integridad Pública, riesgos fiscales y riesgos de seguridad de información, así como otros marcos y normatividad aplicable, dependiendo del sector al cual pertenece la entidad, especialmente aquellos requerimientos definidos por las instancias de vigilancia dependiendo de la naturaleza y funciones que desarrolla la Corporación, de manera tal que se cuente con toda información necesaria para la identificación, análisis y valoración de riesgos, con un enfoque integral.

Los ámbitos que se involucran en la gestión del riesgo, con sus elementos comunes que corresponden al análisis del contexto estratégico interno y externo, la definición de la política para la gestión integral del riesgo y los pasos metodológicos aplicables de i) identificación y descripción del riesgo, ii) análisis del riesgo inherente, iii) diseño y análisis de controles y iv) valoración del riesgo residual, generales para todas las tipologías de riesgo que desarrolla la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025) del DAFP, los cuales se despliegan de forma detallada en la siguiente gráfica:

Figura 13 Articulación ámbitos gestión del riesgo



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

El análisis integral de los riesgos contempla aquellos eventos que puedan afectar el cumplimiento de las funciones y objetivos institucionales, incluyendo:

- La afectación al patrimonio público y la sostenibilidad financiera.
- La vulneración de activos de información y sistemas tecnológicos.
- La pérdida de confianza por parte de usuarios, comunidades, entes de control y demás partes interesadas.
- Conductas asociadas a corrupción, fraude o incumplimiento ético que comprometan la integridad del servicio público.

La política adopta un enfoque transversal, aplicable a todas las tipologías de riesgo que afectan a la Corporación, y se desarrolla mediante los siguientes pasos metodológicos:

Identificación y descripción del riesgo:

- Reconocimiento de eventos potenciales que puedan afectar los procesos misionales, estratégicos o de apoyo.
- Definición clara del riesgo, sus causas, consecuencias y factores asociados.

Análisis del riesgo inherente:

- Evaluación de la probabilidad y el impacto del riesgo en ausencia de controles.
- Determinación del nivel de severidad inicial.

Diseño y análisis de controles:

- Identificación de medidas existentes o propuestas para mitigar el riesgo.
- Evaluación de su eficacia, cobertura, oportunidad y trazabilidad.

Valoración del riesgo residual:

- Recalificación del riesgo considerando la efectividad de los controles aplicados.
- Determinación del nivel final de exposición y definición de acciones de tratamiento.

IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

Los riesgos identificados deben tener impacto en el cumplimiento de objetivos estratégicos, estar alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos. Para su adecuada formulación, deben contener unos atributos mínimos, para lo cual se puede hacer uso de las características SMART:

De acuerdo con lo anterior, se debe tener en cuenta que los indicadores del Sistema Integrado de Gestión- SIG-C, permiten medir el cumplimiento del objetivo de cada proceso, alineados con la plataforma estratégica del SIG-C (Objetivos, política, misión y visión) y de la misma manera los riesgos se identifican a partir de los factores de riesgo que puedan afectar el cumplimiento del objetivo de cada proceso.

La identificación de riesgos se realiza bajo un enfoque sistemático, transversal a toda la entidad, asegurando una base sólida para el análisis, tratamiento y seguimiento efectivo de los riesgos institucionales.

Fuentes generadoras del Riesgo: las fuentes generadoras de riesgos son circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

Tabla. Fuentes Generadoras de Riesgo

Factor	Definición		Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional		Falta de aplicación de los procedimientos
			Falta segregación de funciones
			Errores de grabación, autorización
			Falta de supervisión o interventoría
Transacción u Operación (aplica para LA/FT/FP	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.		Contrapartes de la entidad (naturales o jurídicas)
			Productos (bienes o servicios) que oferta/requiere
			Canales utilizados para la operación
			Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.		Fraude Interno
			Soborno
			Gestión inadecuada de conflicto de Intereses
			Corrupción

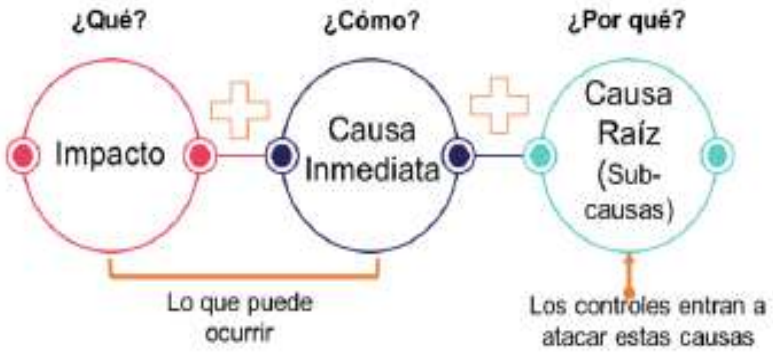
Factor	Definición		Descriptores
			Hurto activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de sistemas de información y aplicaciones
			Caída de redes
			Errores en hardware o software
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.		Fraude Externo
Factor	**Definición**		**Descriptores**
			Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades Públicas Versión 7 de 2025

Descripción del Riesgo

La descripción del riesgo se realiza a partir de los documentos que establecen el direccionamiento estratégico de la Corporación Autónoma Regional del Cesar, identificando aquellos eventos o situaciones que puedan afectar el normal desarrollo de los objetivos estratégicos o de los procesos institucionales.

Cada riesgo debe ser descrito de manera completa, clara y comprensible, de tal forma que permita su entendimiento tanto por los líderes de proceso como por personas ajenas al mismo, garantizando la consistencia en su análisis y gestión. La redacción debe iniciar con la frase: "POSIBILIDAD DE", seguida de la situación o evento que podría impactar la entidad, permitiendo estandarizar la información y facilitar su priorización y seguimiento.



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Impacto: las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la organización la materialización del riesgo.

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

Estos dos elementos permiten plantear el evento no deseado (¿qué puede ocurrir?), es decir la situación, acción, condición o suceso incierto que, si ocurre, podría afectar el logro de los objetivos de la entidad.
Características clave: Debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar.

Causa raíz: Se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles en el paso 3 de diseño y análisis

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

Análisis de Riesgo Inherente

Determinar la probabilidad:

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

Algunas actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Muy Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

La exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año; se establecen los criterios para definir el nivel de probabilidad así:

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 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 más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Determinación del Impacto

Son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en versiones anteriores de la guía se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se hace necesario agruparlos en impacto económico y reputacional, con el fin de facilitar el análisis y evitar la subjetividad en los análisis por parte de los líderes internos.
En la siguiente tabla se establecen los criterios para definir el nivel de impacto:

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

Fuente: Actualizada Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, los cuales tienen diferentes niveles, se debe tomar el más alto

Análisis de severidad

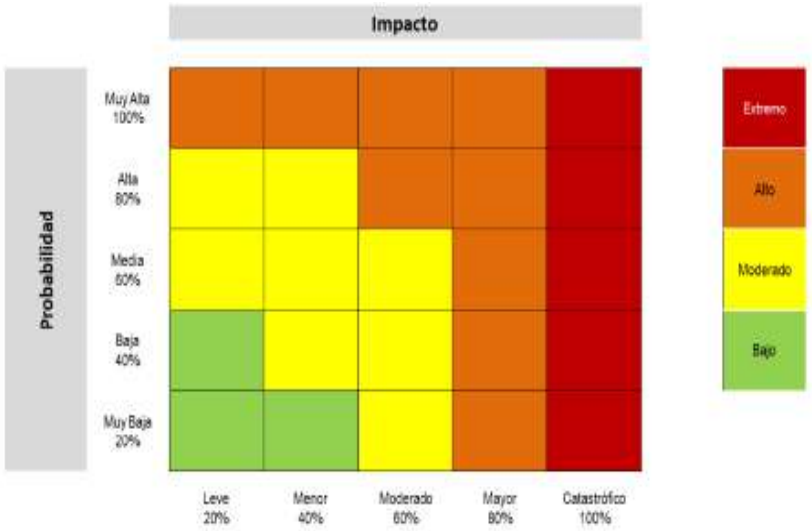
Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor

Análisis Preliminar (Riesgo Inherente)

En esta fase, una vez que el riesgo ha sido identificado y descrito, se procede a evaluar sus características mediante el análisis de dos variables fundamentales: la probabilidad de ocurrencia y el impacto potencial. A partir del análisis de la probabilidad de ocurrencia del

riesgo y sus consecuencias o impactos, se busca determinar el nivel de RIESGO INHERENTE.

Para la determinación del nivel de severidad del riesgo inherente, se definen cuatro (4) zonas de severidad como se observa en la matriz de calor que se presenta a continuación:



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Diseño y análisis de los Controles

Las actividades de control son acciones concretas y con unos atributos específicos que son establecidas a través de políticas, procedimientos u otras directrices o documentos institucionales e implementados con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos. Para la identificación o bien el diseño de controles se debe tener en cuenta que:

Estas se pueden diseñar y establecer para cada riesgo a través de diferentes mecanismos, bien sea a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos que el líder del proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo.

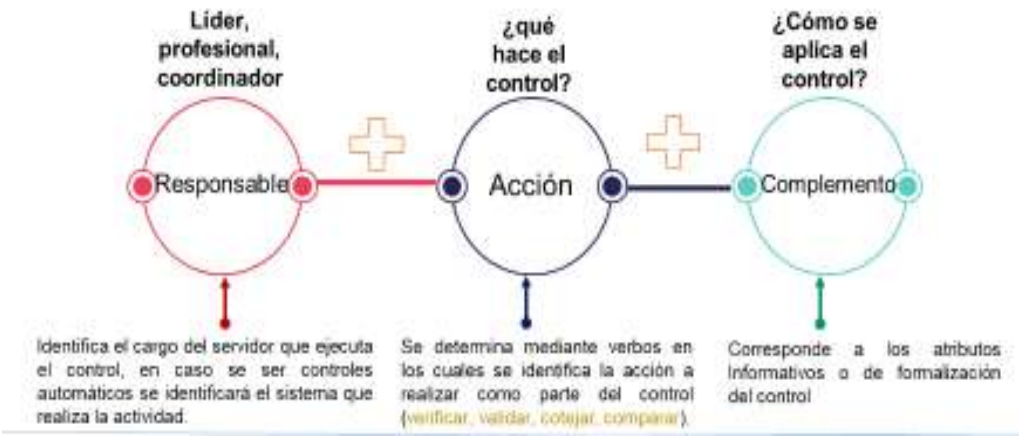
Se requiere considerar los diferentes atributos de las actividades de control para asegurar aspectos tales como: los responsables de su ejecución, la segregación de funciones y niveles de autoridad apropiados.

Estructura para la descripción del control

Para una adecuada redacción del control se propone una estructura que facilitara más adelante entender su tipología y otros atributos para su valoración.

La estructura es la siguiente:

Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en caso se ser controles automáticos se identificará el sistema que realiza la actividad.
Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
Complemento: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado.



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

Tipologías de Controles:

Con el fin de establecer la tipología de controles para su posterior validación, es necesario acudir al ciclo de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo, o bien una combinación de estos.

A continuación, podemos observar la gráfica que describe la Cadena de valor del proceso y las tipologías de controles:

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional, 2025.

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

<u>Valoración de Controles</u>:

La Corporación Autónoma Regional del Cesar - CORPOCESAR establece los controles considerando tres aspectos clave: la estructura para su descripción, la tipología del control y la forma en que este es implementado.

Es fundamental tener en cuenta que los controles preventivos y detectivos contribuyen principalmente a la reducción de la probabilidad de ocurrencia del riesgo, mientras que los correctivos suelen estar orientados a la mitigación del impacto una vez materializado el evento; por tal razón, es indispensable evaluar qué tipo de controles deben ser definidos o fortalecidos para mitigar adecuadamente los riesgos identificados dentro de los procesos de la entidad.

Adicionalmente, debe aclararse que, según su tipología (preventivo, detectivo o correctivo) y su modo de implementación (manual o automático), a cada control se le asigna un peso porcentual. Este peso es un insumo fundamental para realizar la valoración del riesgo inherente.

A continuación, se establecen los criterios para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización ***es de aclarar que mínimo se deben garantizar la tipología y la implementación del control para conocer la***

eficiencia de este y los otros atributos se determinan bajo el criterio del líder del proceso de manera informativa.

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
***Implementación** *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional, 2020.

Para la Descripción del Control no se aplica valoración, pero deben analizarse para garantizar su el diseño, como los aspectos siguientes:

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
	Combinación estructuras documentales y sistemas de información	Se aplican análisis documentales y registros en sistemas de información de apoyo.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
	Combinado (manual y electrónico)	

Características de Eficiencia		Descripción
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional, 2025.

Valoración del riesgo (riesgo residual):

Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

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

En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

Consolidación Mapa de Riesgos Integral

Una vez aplicada la totalidad de la metodología explicada se procede con la elaboración de los mapas de riesgo por proceso, cuya estructura puede corresponder a una matriz en formato Excel como la que se viene manejando en CORPOCESAR.

ESTRATEGIAS PARA COMBATIR EL RIESGO

Las estrategias para enfrentar un riesgo identificado se basan en tres posibles decisiones: aceptarlo, reducirlo o evitarlo. La elección de una de estas alternativas depende del nivel de riesgo evaluado. Para los procesos en funcionamiento, dicha evaluación se realiza sobre el riesgo residual; en el caso de procesos nuevos, se analiza a partir del riesgo inherente.

Cada estrategia seleccionada debe estar respaldada por un plan de acción específico, el cual debe ser incorporado en el mapa de riesgos correspondiente. Este plan de acción permite gestionar adecuadamente el riesgo, garantizando su seguimiento y control, y asegurando la trazabilidad de las decisiones tomadas.

MONITOREO Y REVISION

El monitoreo y la revisión del riesgo se fundamentan en el Modelo Integrado de Planeación y Gestión (MIPG), específicamente en su dimensión 7, la cual incorpora el Modelo Estándar de Control Interno (MECI). Este modelo, junto con el enfoque de las líneas de defensa, actúa como eje articulador para definir y distribuir las responsabilidades relacionadas con la gestión del riesgo y el control interno.

Estas responsabilidades no recaen en una única dependencia, sino que están distribuidas entre diferentes servidores de la entidad, según su rol dentro de la estructura organizacional, garantizando así un enfoque integral y coordinado para la administración del riesgo.

Los monitoreos le corresponden a: la línea estratégica, primera y segunda línea de defensa y se desarrollarán de la siguiente manera:

Línea estratégica: el comité de Coordinación de Control Interno realizará monitoreo cada semestre, para verificar el cumplimiento de la política de administración de riesgos. Estos se reportarán a través de los (formatos, herramientas y/o instrumentos que los responsables determinen).

Primera línea de defensa: Realiza monitoreo cuatrimestral a las acciones tendientes a controlar y gestionar los riesgos y enviará a la Subdirección General Área de Planeación los resultados de esos monitoreos los 5 primeros días hábiles siguientes al cierre del periodo antes descrito. Estos se reportarán a través de los formatos, herramientas y/o instrumentos que los responsables determinen.

Sumado a lo anterior, la primera línea de defensa debe monitorear los riesgos y revisar la efectividad y el desempeño de las herramientas implementadas para su gestión. Para lo cual, debe:

- ✓ Asignar responsables
- ✓ Fijar fechas de inicio y terminación de las actividades requeridas
- ✓ Señalar la forma de seguimiento (encuestas, muestreos aleatorios de calidad, u otros)
- ✓ Definir la periodicidad de revisión
- ✓ Documentar las actividades de monitoreo

Segunda línea de defensa: Realizará monitoreo cuatrimestral a través de los informes que los líderes de procesos remitan, asegurando que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados, se ejerzan por el responsable apropiadamente y funcionen como se pretende. Estos se reportarán a través de los formatos, herramientas y/o instrumentos que los responsables determinen.

GESTIÓN PREVENTIVA DE RIESGOS FISCALES

Este apartado tiene como finalidad orientar el análisis de la operación de las entidades públicas para identificar y gestionar los riesgos que puedan provocar un daño patrimonial al Estado, el cual en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado. Para ello, es necesario partir del concepto de gestión fiscal, que incluye los siguientes componentes:

¿Qué es?	¿Quién la realiza?	¿Qué comprende?	¿Para qué?
El conjunto de actividades económicas, jurídicas y tecnológicas	Los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos	La adecuada y correcta • adquisición • planeación • conservación • administración • custodia • explotación • enajenación • consumo • adjudicación • gasto • inversión • disposición (de los bienes públicos) • recaudación • manejo • inversión (de sus rentas)	En orden a cumplir los fines esenciales del Estado, con sujeción a los principios establecidos en artículo 3 de la Ley 610 de 2000

Fuente: Elaboración Dirección de Gestión y Desempeño. 2025. Con base en Ley 610/2000 art. 3.

A partir de lo anterior, el control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante el cual tiene carácter excepcional, no vinculante, no implica coadministración, no versa sobre la conveniencia de las decisiones de los administradores de recursos públicos, se realiza en forma de advertencia al gestor fiscal y deberá estar incluido en un sistema general de advertencia público; se busca con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, con lo cual surgen conceptos clave que se desarrollan a continuación.

Control fiscal interno y prevención del riesgo fiscal:

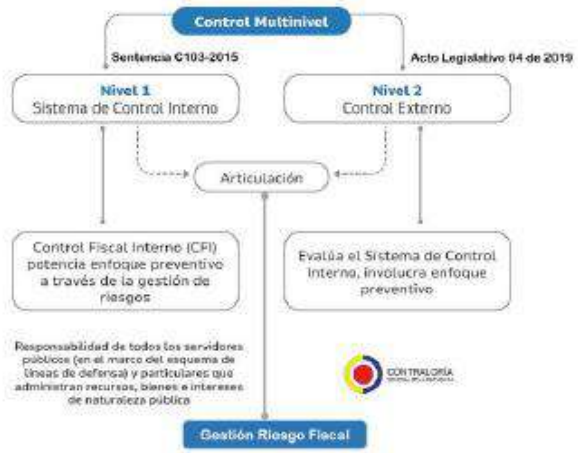
En el nuevo modelo constitucional, el control fiscal adquiere un enfoque preventivo que se potencia con el control interno, a partir de la premisa que el Sistema de Control Interno es el conjunto de mecanismos y medidas que toma una administración para proveer una seguridad razonable respecto al logro de los resultados, con lo cual se brinda también seguridad razonable al gestor fiscal, de haber tomado todas las medidas posibles para evitar daños al patrimonio del Estado.

La denominación de **gestor fiscal** comprende los jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores de proyectos, responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros roles cuyas funciones u obligaciones incidan en la gestión fiscal.

Se define entonces un modelo de **control fiscal multinivel**, entendido como la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

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

La siguiente figura muestra la Articulación del modelo constitucional control fiscal y el sistema de control interno:



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

A continuación, se presenta el paso a paso de la gestión del riesgo fiscal (identificación, análisis del riesgo inherente, control y valoración del riesgo residual), que debe vincularse al análisis general de los riesgos institucionales de la Corporación Autónoma Regional del Cesar - CORPOCESAR, a fin de contar con un esquema integral que facilite su seguimiento por parte de los líderes del proceso.

La metodología que se propone es de gran utilidad para gestionar de manera efectiva los recursos, bienes e intereses patrimoniales de naturaleza pública, con el fin de prevenir efectos dañosos, lo cual a la vez permite mitigar la posibilidad de afectación al patrimonio por parte de los diferentes gestores fiscales.

Definición y elementos del riesgo fiscal:

El riesgo fiscal se define de la siguiente manera:

> Efecto dañoso sobre recursos, bienes y/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 dañoso: es el daño que se generaría sobre los recursos, 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, los bienes y/o los intereses patrimoniales de naturaleza pública.

Lo anterior se puede resumir de la siguiente manera:

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

Nota: *No se debe confundir el riesgo fiscal con el daño patrimonial. El riesgo fiscal se relaciona con el evento de potencial efecto perjudicial sobre los recursos, bienes o intereses públicos, mientras que el daño patrimonial es la afectación real y concreta a los mismos, como resultado de una acción u omisión*.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional, 2025.

Metodología para el levantamiento del mapa de riesgos fiscales

A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, fundamental para la protección de los recursos, bienes e intereses patrimoniales públicos a cargo de los gestores fiscales (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros), lo cual contribuye al cumplimiento de sus funciones y al aseguramiento razonable para la toma de decisiones.

Paso 1 identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

Para las **circunstancias inmediatas**, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas

Para identificar los **puntos de riesgo y las circunstancias inmediatas**, se tendrán en cuenta los aportes de personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar al análisis crítico y objetivo de la gestión fiscal de la Corporación. A continuación, se presentan unas preguntas que sirven para identificar puntos de riesgo fiscal y circunstancias inmediatas:

Criterio para la identificación	Sirve para identificar
¿En qué procesos de la entidad se realiza gestión fiscal?	Puntos de riesgo fiscal
Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. **Nota 1**: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. **Nota 2**: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. **Nota 3**: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. **Nota 4**: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.	Puntos de riesgo fiscal y circunstancias inmediatas
En un ejercicio autocrítico, realista y objetivo, ¿cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? **Nota:** Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.	Circunstancias inmediatas

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 de 2025

Identificación de áreas de impacto

En el contexto del riesgo fiscal, el área de impacto se refiere siempre a una consecuencia de carácter económico que afecta al patrimonio público.

Esto implica que, en caso de materializarse el riesgo, la Corporación Autónoma Regional del Cesar - CORPOCESAR estaría expuesta a una pérdida o afectación directa sobre sus recursos financieros o bienes, comprometiendo así su sostenibilidad, eficiencia y responsabilidad en el uso de los recursos públicos.

Es importante tener en cuenta que no todos los efectos económicos constituyen riesgos fiscales; sin embargo, todo riesgo fiscal implica necesariamente un efecto económico.
Esto se debe a que el riesgo fiscal se define como aquel que conlleva un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Por lo tanto, mientras pueden existir efectos económicos derivados de riesgos operativos, reputacionales u otros que no comprometan directamente el patrimonio público, todo riesgo fiscal representa una amenaza directa al patrimonio económico de la entidad.

Son ejemplos de efectos económicos que no constituyen riesgos fiscales, los siguientes.

✓ Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.

✓ Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público.

✓ Existencia de actuación de cobro coactivo por parte de la entidad.

✓ Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.

✓ Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su “normal uso” (máquinas eléctricas, computadores, celulares, etc.).

Identificación de la Causa Raíz o Potencial Hecho Generador

La Causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República).

La Causa raíz o potencial hecho generador y el efecto dañoso (daño) mantienen entre sí una relación directa de causa y efecto. En este sentido, la identificación de la causa raíz o del potencial hecho generador del riesgo fiscal se logra a través del análisis de la acción, omisión o acto que pueda lesionar el patrimonio estatal.

Una adecuada gestión de riesgos fiscales exige que la identificación de las causas sea objetiva, rigurosa y fundamentada. Esto se debe a que los controles que se diseñen e implementen deben estar orientados a mitigar o eliminar dichas causas, ya que son el origen del riesgo fiscal. Solo mediante un análisis preciso de las acciones, omisiones o condiciones que pueden generar un daño patrimonial, es posible estructurar controles efectivos que permitan prevenir la materialización de daños fiscales y proteger los recursos públicos.

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

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho.

Descripción del Riesgo Fiscal.

A continuación, se presenta la estructura de redacción de riesgos fiscales, la cual integra los elementos clave previamente descrito. así mismo, se presentan algunos ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

Para redactar un riesgo fiscal se debe tener en cuenta:

✓ Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
✓ Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
✓ Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica causa raíz- para que se presente el riesgo.
✓ Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

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

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

Ejemplo para la Corporación Autonoma Regional del Cesar – CORPOCESAR:

Proceso: Gestión Financiera

Objetivo: Administrar adecuadamente los recursos financieros de la Corporación a través de la verificación, seguimiento y control de las actividades relacionadas con el presupuesto, tesorería, pagaduría y contabilidad para proveer información útil para la toma de decisiones.

Alcance: Comprende desde la etapa de planeación presupuestal, presentación de informes financieros, hasta la administración de los recursos financieros de la Entidad.

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de pérdida o disminución de recursos	por prescripción de los términos para el recaudo de obligaciones ambientales en mora	a causa de debilidades en la gestión y/o ejecución de los procedimientos de cobro persuasivo y coactivo.

Conclusión: El riesgo fiscal existe desde el momento en que, existiendo obligaciones en mora, los procedimientos de cobro no se ejecutan de manera oportuna y correcta, pues allí surge la potencial reducción del recaudo. En esta etapa, el sistema de control interno debe ser capaz de tomar los correctivos necesarios, pues una vez se materialice la prescripción, se configura el daño patrimonial (hallazgo fiscal) a partir del cual el órgano de control fiscal procede a establecer y exigir la responsabilidad del gestor fiscal.

Paso 2 Valoración del riesgo fiscal

En esta etapa se realiza la **Evaluación de riesgos** que busca establecer el nivel de riesgo inherente, entendido como la probabilidad de ocurrencia del riesgo, así como su impacto en la gestión fiscal. Se aplican los lineamientos para la redacción del control establecidos en los apartados iniciales de la Política.

Probabilidad: La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.
Impacto: Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso recae sobre un bien, recurso o interés patrimonial de naturaleza pública. Toda potencial consecuencia económica sobre el patrimonio público es relevante, sin embargo, existen niveles para su valoración.
Determinación del nivel de riesgo inherente: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad.

Paso 3 Valoración de los Controles

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

Tipologías de controles: ✓ Control Preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete. ✓ Control Detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
✓ Control Correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos.
Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Se aplican los lineamientos para la redacción del control establecidos en los apartados iniciales de la Política.

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

RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCION

La Corporación Autónoma Regional del Cesar - CORPOCESAR, adopta como marco de referencia para la gestión del riesgo de corrupción los lineamientos establecidos en la versión 4 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas (2018), expedida por el Departamento Administrativo de la Función Pública. Esta guía continúa vigente y constituye un instrumento técnico clave para la identificación, análisis, evaluación, tratamiento, monitoreo y seguimiento del riesgo de corrupción en las entidades del Estado.

En consecuencia, la formulación del mapa de riesgos de corrupción deberá remitirse a los parámetros establecidos en dicho documento. Con el fin de facilitar su aplicación, a continuación, se transcriben algunas de las pautas más relevantes contenidas en la Guía, las cuales deben ser tenidas en cuenta durante todo el proceso de gestión del riesgo.

Adicionalmente, se informa que, de acuerdo con información disponible, la Secretaría de Transparencia se encuentra actualmente analizando la posibilidad de actualizar la metodología para la gestión de riesgos de corrupción. No obstante, hasta tanto se expidan nuevos lineamientos oficiales, se mantiene la aplicación obligatoria de la Guía de 2018.

RIESGO DE CORRUPCION

Definición

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCION U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO

El riesgo de la Corrupción se establece sobre Procesos.

El riesgo debe estar descrito de manera clara y precisa. 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 entre un riesgo de gestión y uno de corrupción, CORPOCESAR utiliza la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

Valoración del Riesgo

Cálculo de la probabilidad e impacto

Análisis de la probabilidad

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

Criterios para Calificar la Probabilidad:

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 Gestión Integral del Riesgo en Entidades Públicas en entidades Publicas

Análisis del Impacto

Para la Determinación del Impacto, CORPOCESAR, el Impacto lo analizará y calificará a partir de las consecuencias identificadas en la fase de descripción del riesgo-

Criterios para calificar el impacto en riesgos de corrupción:

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Nivel de impacto MAYOR

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 de 2025

Análisis del riesgo del Impacto de Corrupción.

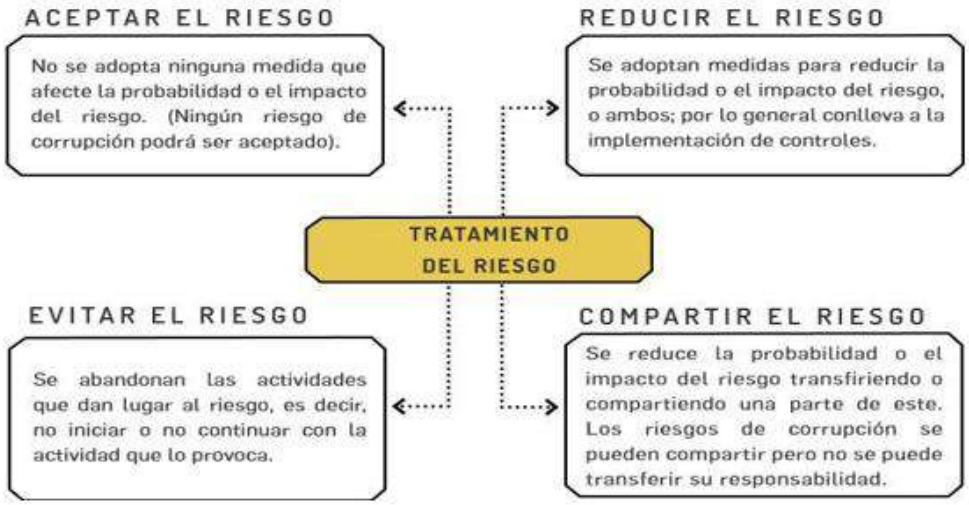
Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Valoración de los Controles

La Corporación Autónoma Regional del Cesar – CORPOCESAR, tendrá en cuenta para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas en entidades públicas, de 2018, continúan vigentes.

Tratamiento del Riesgo.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:



Fuente: **Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 de 2025**

El tratamiento de control es rol de la primera línea como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.

Fuente: **Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 de 2025**

Monitorio de Riesgo de Corrupción.

Los líderes de proceso, en conjunto con sus equipos de trabajo deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de Planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Reporte de la gestión del riesgo de corrupción

La Corporación Autónoma Regional del Cesar - CORPOCESAR deberá reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

Seguimiento de Riesgo de Corrupción

El jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la Página web de la entidad.

Acciones a seguir en caso de materialización del Riesgo de Corrupción

En el evento de materializarse el riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

✓ Informar a las autoridades de la ocurrencia del hecho de corrupción.
✓ Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
✓ Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
✓ Llevar a cabo un monitoreo permanente.

La oficina de Control Interno deberá asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

✓ Determinar la efectividad de los controles
✓ Mejorar los controles
✓ Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
✓ Determinar si se adelantaron acciones de monitoreo.

RIESGO DE SEGURIDAD DE LA INFORMACION

El Modelo de Seguridad y Privacidad de la Información es un instrumento desarrollado por el Ministerio de las Tecnologías de la Información y de las Comunicaciones que imparte los lineamientos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información basado en las normas y estándares de mejores prácticas en materia de seguridad de la información.

Este capítulo aborda temas como la identificación de activos de información, riesgos, amenazas y vulnerabilidades, para llevar a cabo un análisis de los riesgos de seguridad de la información, luego, la implementación de controles diseñados para mitigar estos riesgos y el proceso de reporte de estos.

A continuación, se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la Disponibilidad, Integridad y Confidencialidad de los activos de información que permiten cumplir con la misión y alcanzar la Visión de la Entidad.

Identificación de los Activos de Seguridad de la Información

En primer lugar, se deben identificar los activos de Información mediante las actividades descritas en los “Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional” del MSPI, en esta se presenta los lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación y clasificación de activos de información de cada entidad.

Pasos para la identificación de los activos:

Como base para la identificación de los riesgos de seguridad de la información se debe tomar el índice de activos de información del proceso.

Para llevar a cabo la identificación de activos, se deberá consultar la sección 3.1.6 del ‘Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 de 2025

Identificación del Riesgo

Posteriormente a la identificación de los activos de la información se deberá o se podrá identificar los riesgos inherentes de seguridad de la información.
Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles **amenazas y vulnerabilidades** que podrían causar su materialización:

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

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

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)

Tipo	Vulnerabilidades
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

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

Descripción del Riesgo:

En este campo se describe la situación específica que da como resultado el correspondiente riesgo. “Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.” Si requiere información adicional remitirse al punto 3.4 de esta misma guía.
Clasificación del Riesgo: Este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad.

Análisis del Riesgo INHERENTE

La determinación de la probabilidad se debe llevar a cabo de acuerdo con lo establecido anteriormente en la presente política, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

Las variables confiabilidad, integridad, y disponibilidad se definirán de acuerdo al modelo de seguridad y privacidad de la información de la estrategia de gobierno digital (GD) del Ministerio de Tecnología de la Información y las Comunicaciones.

Frecuencia: Este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.
% Probabilidad Inherente: Este campo corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa.

Probabilidad inherente: Este campo corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa.

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 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 más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Determinar el impacto

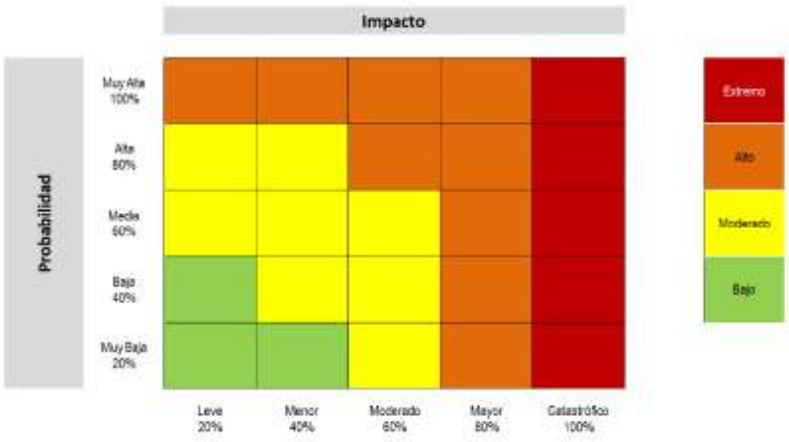
En esta actividad se debe realizar el análisis del impacto de la materialización de estos riesgos

% Impacto Inherente: Este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa
Impacto Inherente: Este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa.

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

Análisis de severidad

Zona de riesgo inherente: En este campo se determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto.



Controles Asociados a la seguridad de la Información

La Corporación Autónoma Regional del Cesar – CORPOCESAR, adoptará para mitigar o tratar los riesgos de seguridad de la información utilizando, como mínimo, los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013. Estos controles están incluidos en el 'Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas', siempre que sean coherentes con los resultados del análisis de riesgo.

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

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas -Versión 7 de 2025

SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA -SIGRIP

Teniendo en cuenta la expedición de la Ley 2195 de 2022, que hace obligatorio para las entidades públicas la "prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional" (artículo 31), la Secretaría de Transparencia de la Presidencia de la República sugiere a las entidades obligadas a implementar un Programa de Transparencia y Ética Pública contar con un sistema de gestión que le permita prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), de manera integral. Para eso, ha diseñado el Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP.

Integridad pública: Las organizaciones se exponen frecuentemente a que sus objetivos no se cumplan como consecuencia de los diferentes intereses que pueden confluir en la toma de decisiones, en la medida que se privilegian intereses propios sobre el interés general de la organización. En el caso del sector público, el interés general, que no es otra cosa que el interés por la consecución de los fines del Estado, también se puede ver afectado por intereses particulares, lo que termina afectando la capacidad de las entidades públicas para cumplir con las funciones que se le han encomendado.

Amenazas para la integridad pública

La Organización para la Cooperación y el Desarrollo Económico, ODCE, ha planteado la necesidad de aplicar un enfoque basado en riesgos cuando se habla de integridad pública. Hay varias amenazas que pueden incidir en diferentes puntos de los procesos organizacionales que terminan afectando la capacidad de una entidad para alcanzar sus objetivos, en particular, asegurar el cumplimiento de la ley.

Para el propósito de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 de 2025, nos centraremos en cinco amenazas para la integridad, que constituyen una lista enunciativa, en la medida que una entidad pública podría identificar adicionales:

Soborno

El Soborno puede ser entendido como "ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]". Y opera en dos niveles: Soborno Entrante y Saliente. Se entiende como Entrante el soborno al servidor de la Entidad, y como Saliente el soborno por parte de servidores a otros en nombre de la Entidad.

Fraude

El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.
Este puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima. El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.

Inadecuada gestión del conflicto de intereses:

Un conflicto de intereses surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.

Corrupción

La Corrupción es “todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral”.

Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP

La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la capacidad del Estado para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento.

El SIGRIP busca articular la Política para la Gestión Integral de Riesgos que formule cada entidad, mediante la cual se gestionan los Riesgos Generales de la Gestión, la Gestión Preventiva de Riesgos Fiscales y los Riesgos de Seguridad de la Información, con los demás elementos que son necesarios para gestionar los riesgos para la integridad pública, que se describen a continuación. Al final, un riesgo de gestión, un riesgo fiscal o un riesgo de seguridad de la información puede tener como causa el soborno, el fraude, un conflicto de intereses gestionado inadecuadamente o la corrupción. Además, puede también favorecer el lavado de activos, la financiación del terrorismo o la financiación de la proliferación de armas de destrucción masiva. Por esta razón, es necesario abordar los riesgos para la integridad pública de forma integral y en estrecha articulación con la gestión institucional del riesgo.

El SIGRIP, además, permite a las entidades dar cumplimiento a los lineamientos establecidos para la gestión de riesgos en los Programas de Transparencia y Ética Pública, según lo dispuesto por la Secretaría de Transparencia de la Presidencia de la República. En la medida que se implemente plenamente el Sistema, la entidad estará acreditando la gestión de riesgos para la integridad pública, de riesgos LA/FT/FP, canales de denuncia y debida diligencia.

Tabla. Roles y Responsabilidades SIGRIP

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	Auditor del Programa	Administrador del Programa	Ejecutores del Programa
Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno	Oficina de Control Interno, Auditoría Interno o quien haga sus veces	Dependencia o persona designada por la Alta Dirección	Directivos, líderes de proceso, servidores y colaboradores
Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.	En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP asume la función de cumplimiento que se desarrolla en el numeral 6.3.7.3	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Planificación

Según lo establecido en esta Guía, las entidades en el marco de la formulación de la Política para la Gestión Integral de Riesgos deberán definir un objetivo y un alcance, así como establecer marco de apetito del riesgo, y el esquema metodológico que aplicarán para lo cual deberán contemplar los siguientes aspectos relevantes del SIGRIP:

Se debe asegurar que dentro del objetivo se contemple la protección de la integridad pública, el alcance de la Política debe contemplar los aspectos relevantes de la organización que se hayan identificado del análisis del contexto interno y externo.

Para el diseño del esquema metodológico, tener en cuenta los lineamientos desplegados a detalle:

Apoyo

Para que el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP pueda operar adecuadamente, la entidad debe disponer de los recursos necesarios, señalar claramente los atributos comportamentales que se requieren, disponer de una estrategia de formación y de comunicación, y documentar cada una de las actividades que se ejecuten; para lo cual:

La entidad debe identificar los recursos financieros y humanos, soluciones de TI, habilidades especializadas, infraestructura organizacional, material de referencia y experiencia que dispone.

Establecer en la Política para la Gestión Integral de Riesgos las características que debe cumplir las personas que realicen un trabajo que afecte el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, su desempeño y operaciones.

La entidad debe asegurar la toma de conciencia del personal, los líderes, el administrador, la Alta Dirección y, en general, de toda la organización, sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.
La toma de conciencia sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, también implica comunicar interna y externamente los resultados de su operación, así como cualquier actualización del Sistema o de algunos de sus elementos. Cada uno de los elementos del Sistema debe estar correctamente documentado.

Operación

Como se indició previamente, el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP es un conjunto de elementos que operan e interactúan entre sí. El principal elemento del Sistema es la Política para la Gestión Integral de Riesgos, que cada entidad debe formular, junto con su respectivo mapa de riesgos.

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos

En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, la entidad deberá identificar y valorar los riesgos que pueden impactar el ejercicio íntegro de la función pública, incluidos los riesgos de LA/FT/FP. La Corrupción es la principal amenaza para la integridad, sin embargo, hay manifestaciones muy específicas de esta práctica que requieren ser identificadas y valoradas individualmente, como lo es el soborno, el fraude y la inadecuada gestión del conflicto de intereses. También, los riesgos por conductas que permiten o favorecen el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva, deben ser gestionados.

Paso 1: Identificación y descripción del riesgo

1. Respecto de la “Identificación de los puntos de riesgo” En el marco de la gestión del riesgo de LA/FT/FP, debe tenerse en cuenta que los puntos de riesgo se refieren a operaciones que lleva a cabo la entidad. Estas operaciones son los puntos de riesgo relevantes, que deben tenerse en cuenta para la identificación del riesgo de lavado de activos, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.

Respecto del riesgo de Corrupción y sus manifestaciones específicas como soborno, fraude e inadecuada gestión del conflicto de intereses, los puntos de riesgos pueden ser cualquier actividad dentro del flujo de proceso y no solo las operaciones.

Respecto de la “Identificación de áreas de impacto” En el marco de la gestión de los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

Respecto de la “Identificación de factores de riesgo” Como factores del riesgo LA/FT/FP se tiene a las contrapartes, los productos, los canales y las jurisdicciones, aspectos mínimos a contemplar en cualquier análisis, los cuales en conjunto conforman el concepto de “transacción” u “operación”, en el entendido que una transacción, en todos los casos, será realizada por un cliente o usuario, que accedió o entregó un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica. Estos factores deben permitirle a la entidad mayor efectividad en el conocimiento de las contrapartes, el diseño y aplicación de señales de alerta, la identificación de operaciones inusuales y la determinación y el reporte de operaciones sospechosas.

Respecto de la “Descripción del riesgo” La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en la Guía. Todos iniciarán con la formula “Posibilidad de”, y deben señalar el impacto, la causa inmediata y la causa raíz.

En el caso particular del riesgo LA/FT/FP, debe hacerse referencia particularmente a las actividades del flujo de procesos en que existe la vulnerabilidad o exposición al riesgo.

Tabla. Ejemplos de análisis de riesgos

Impacto	Causa inmediata		Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar [...]”.	
	Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una	

Impacto	Causa inmediata		Causa raíz
		persona actúe o se abstenga de actuar [...]".	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Paso 2: Análisis de Riesgo Inherente

Respecto del "Análisis de Riesgo Inherente" Por la naturaleza de los riesgos para la integridad pública, el objetivo fundamental es prevenirlos, detectarlos y reportarlos en términos de oportunidad y eficacia. Esta perspectiva debe ser transversal al análisis del riesgo y al diseño de controles.

Paso 3: Diseño y Análisis de Controles

Respecto del "Diseño y análisis de controles" Para el diseño de controles deberá tenerse en cuenta que, además de la Política para la Gestión Integral de Riesgos y su respectivo Mapa de Riesgos, las entidades deberán desarrollar, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, un Manual para el desarrollo del principio de debida diligencia, contar con una función de cumplimiento y formular una serie de herramientas de gestión.

Paso 4: Valoración de Riesgo Residual

Debida diligencia en el conocimiento de las contrapartes: Las entidades deben contar con lineamientos y procedimientos internos sobre la debida diligencia con que deben llevar a cabo el conocimiento de sus contrapartes.

De acuerdo con lo anterior, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, cada entidad deberá contar con un Manual que incorpore mecanismos que desarrollen el principio de debida diligencia en todas las interacciones con contrapartes, en las que exista una exposición a riesgos para la integridad pública, es decir, en aquellas interacciones en que se haya identificado un riesgo de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.

Herramientas de gestión del riesgo

Además de contar con una Política para la Gestión Integral de Riesgos, un Mapa de Riesgos y una función de cumplimiento distribuida dentro de la organización, la gestión de riesgos para la integridad pública requiere que la organización implemente una serie de políticas, procedimientos y códigos de conducta, que contribuyen a la integralidad del sistema.

Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP).

La Corporación Autónoma Regional del Cesar – CORPOCESAR, establece como política institucional el compromiso de la Alta Dirección con una cultura de prevención y mitigación del LA/FT/FP; prohíbe y rechaza cualquier practica asociada al LA/FT/FP; CORPOCESAR se obliga a cumplir con la normativa ALA/CFT/CFP; se obliga a actuar con debida diligencia en el conocimiento de las contrapartes; promociona la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias.

Política Antisoborno.

La Corporación Autónoma Regional del Cesar – CORPOCESAR, establece como política institucional el compromiso de la Alta Dirección con una cultura de prevención y mitigación del soborno; prohíbe y rechaza cualquier practica asociada al soborno; obligue a la entidad a cumplir con la normativa antisoborno; CORPOCESAR se obliga a actuar con debida diligencia en el conocimiento de las contrapartes; promociona la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias.

Política Antifraude.

La Corporación Autónoma Regional del Cesar – CORPOCESAR, establece como política institucional el compromiso de la Alta Dirección con una cultura de prevención y mitigación del fraude; prohíbe y rechaza cualquier practica asociada al fraude; CORPOCESAR se obliga a cumplir con la normativa antifraude; promociona la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias.

Procedimiento para la gestión de los conflictos de intereses.

La Corporación Autónoma Regional del Cesar – CORPOCESAR deberá formular un procedimiento interno que, expresamente: contenga un catálogo de situaciones que se podrían presentar dentro de la organización, con ejemplos reales, que generen un conflicto de intereses; el paso a paso que debe seguir cualquier persona para declarar un conflicto de intereses al interior de la organización; el paso a paso que seguirá la entidad para tramitar un conflicto de intereses; el margen de acción de la entidad para gestionar los conflictos de intereses; el paso a paso para realizar las declaraciones periódicas que la ley establezca; el paso a paso para controlar que se hayan realizado las declaraciones periódicas que la ley establece.

Procedimiento para el reporte de operaciones sospechosas.

La Corporación Autónoma Regional del Cesar – CORPOCESAR deberá formular un procedimiento interno que, expresamente: establezca los criterios y señales de alerta para determinar que una operación es inusual; el paso a paso para que los líderes de proceso reporten a quien ostente la función de cumplimiento las operaciones inusuales; el paso a paso para que quien ostenta la función de cumplimiento evalúe la operación inusual y determine si es sospechosa; el paso a paso para reportar a las autoridades competentes la operación sospechosa, incluso cuando fue intentada.

Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético.

La Corporación Autónoma Regional del Cesar – CORPOCESAR deberá formular un procedimiento interno que, expresamente: identifique los medios de recepción de denuncias e inquietudes; el paso a paso para evaluar las denuncias e inquietudes que se presenten por el canal; el paso a paso para tratar las denuncias e inquietudes que correspondan a todas las herramientas de gestión deben desarrollarse en los Programas de Transparencia y Ética Pública de las entidades. La Política para la Gestión Integral de Riesgos, el Mapa de Riesgos, y el Manual de Debida Diligencia en el Conocimiento de las Contrapartes, también, hacen parte integral del Programa de Transparencia.

Monitoreo, evaluación, auditoría y mejora

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto permanente de monitoreo, evaluación, auditoría y mejora. Para este propósito, deben tenerse en cuenta las siguientes consideraciones:

- En la Política para la Gestión Integral de Riesgos debe quedar establecido la periodicidad y el contenido del monitoreo a los riesgos que gestiona el SIGRIP.
- Corresponde al Administrador del Programa, desde su rol como segunda línea de defensa, la evaluación de la gestión del riesgo.

- El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto de auditoría, la cual estará a cargo de la unidad de control interno o quien ejerza la tercera línea de defensa.
- Finalmente, la mejora del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP corresponde a la Alta Dirección o línea estratégica, quien lleva a cabo la revisión integral del Sistema

BIBLIOGRAFÍA

Guía para la Gestión Integral del Riesgo en Entidades Públicas en Entidades Públicas, DAFP, Versión 7, de agosto de 2025 y anexos.