POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

GIT DE PLANEACIÓN
Junio de 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La presente Política de Administración del Riesgo establece los lineamientos y metodologías para identificar, evaluar, mitigar y monitorear los riesgos que puedan afectar la operación y los objetivos de la Contaduría General de la Nación (CGN). Se fundamenta en el Modelo Integrado de Planeación y Gestión (MIPG), la NTC-ISO 31000:2018 y la Metodología General Ajustada (MGA WEB).

Además, se actualiza con los lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - Versión 6, del Departamento Administrativo de la Función Pública (DAFP), incluyendo la gestión del riesgo fiscal, estrategias mejoradas de control y lineamientos de riesgos de seguridad de la información.

2. OBJETIVO

Establecer las directrices y lineamientos para la administración de los riesgos en la Contaduría General de la Nación, con el fin de fortalecer la toma de decisiones, contribuir al cumplimiento de los objetivos estratégicos de la Entidad y promover una cultura organizacional orientada al control y la prevención.

Así mismo, pretende obtener un nivel de riesgo residual aceptable mediante la implementación efectiva de controles y acciones de mitigación.

3. ALCANCE

La política será aplicable en todo nivel, a los procesos institucionales, activos y proyectos, de conformidad con cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y de acuerdo con las correspondientes líneas de defensa. Sobre el particular es importante realizar las siguientes precisiones:

- **Riesgos de gestión:** se presentan en todos los procesos institucionales; están relacionados con eventos que pueden afectar el cumplimiento de las funciones, objetivos y metas de la Entidad. Identificarlos a tiempo permite la acertada toma de decisiones y evitar afectaciones en la operación institucional.

  En línea con lo anterior, se incluye en este alcance a los riesgos institucionales, los cuales corresponden a los riesgos de gestión con un nivel alto o extremo de impacto. Se caracterizan porque pueden comprometer seriamente la sostenibilidad y los objetivos estratégicos de la Entidad, por lo que requieren una atención prioritaria y medidas efectivas de mitigación.

- **Riesgos de corrupción**: aplica a todos los procesos institucionales, se refiere a la posibilidad de que se utilicen el poder o los recursos públicos para fines privados, ya sea por acción u omisión. Su control fortalece la ética, la transparencia y la confianza ciudadana.

- **Riesgos fiscales**: se presentan en todos los procesos institucionales, están relacionados con posibles afectaciones a los recursos públicos o bienes del Estado debido a eventos que generen pérdidas o perjuicios patrimoniales. Su adecuada gestión protege el patrimonio público y asegura su correcto uso.

- **Riesgos de seguridad de la información y seguridad digital**: aplica a todos los activos digitales y sistemas críticos. Se refiere a amenazas que pueden explotar vulnerabilidades y causar pérdidas o daños a la información. Gestionarlos adecuadamente garantiza la integridad, disponibilidad y confidencialidad de los datos institucionales.

- **Riesgos en proyectos**: se presentan en todos los proyectos de inversión registrados en el Banco de Programas y Proyectos de Inversión Nacional (BPIN) del Departamento Nacional de Planeación (DNP), desde su etapa de prefactibilidad. Su identificación temprana facilita una mejor planeación, ejecución y uso eficiente de los recursos.

4. GLOSARIO[1]

- **Activo de información**: en relación con la seguridad de la información, se refiere a cualquier tipo de dato, archivo, documento o recurso digital que tiene un valor para una organización y que debe ser protegido debido a su importancia para el funcionamiento o los objetivos de esta.
- **Amenazas**: causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.
- **Asegurar**: en el marco del Modelo Integrado de Planeación y Gestión (MIPG), se refiere a la garantía de que los procesos, actividades, operaciones y resultados de una entidad pública se realicen de acuerdo con las normas, políticas y planes establecidos. Esto implica la verificación y evaluación objetiva para asegurar la eficiencia, eficacia, transparencia y legalidad de la gestión.
- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

---

[1] Las fuentes de las definiciones de este numeral son las siguientes:
- Guía para la Administración del Riesgo el diseño de controles de entidades públicas, versión 5 y 6.
- https://www.dnp.gov.co/LaEntidad_/subdireccion-general-inversiones-seguimiento-evaluacion/direccion-proyectos-informacion-para-inversion-publica/Paginas/metodologia-general-ajustada-mga.aspx

- **Ciberseguridad**: se refiere a las actividades y medidas necesarias para proteger los activos de información, como la información procesada, almacenada y transportada por los sistemas de información interconectados, los usuarios involucrados y otros afectados por las ciberamenazas.
- **CICCI (Comité Institucional de Coordinación de Control Interno)**: órgano asesor encargado de coordinar y articular el control interno institucional, conforme a lo establecido por el Modelo Integrado de Planeación y Gestión (MIPG).
- **Confidencialidad**: propiedad de la información que la hace no disponible, es decir, que excluye de su divulgación a individuos, entidades o procesos no autorizados.
- **Control**: medida que permite reducir o mitigar un riesgo.
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Gestión del Riesgo**: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Gestión del Riesgo Fiscal**: son las actividades que debe desarrollar la Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales.
- **Integridad**: propiedad de exactitud y completitud de la información. Este principio de seguridad de la información asegura que la información se mantenga íntegra; es decir, que no haya sido alterada, manipulada o dañada de manera intencionada o accidental, y que permanezca exacta y fiable a lo largo del tiempo y en su transmisión o almacenamiento.
- **Impacto**: consecuencias o efectos negativos que puede generar la materialización de un riesgo en los objetivos, procesos o activos de la organización.

- **Metodología General Ajustada (MGA)**: es un método para la formulación y estructuración de proyectos de inversión pública, desarrollada por el Departamento Nacional de Planeación (DNP).
- **Probabilidad**: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
  Nota: los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo Inherente**: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual**: es el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Vulnerabilidad**: debilidad de un activo o control que puede ser explotado por una o más amenazas.

5. NIVELES DE RESPONSABILIDAD PARA EL MANEJO DE LOS RIESGOS

El Modelo Integrado de Planeación y Gestión (MIPG), en la dimensión 7 denominada "Control Interno", establece la gestión del riesgo y el control como una responsabilidad compartida, estructurada a través de una Línea Estratégica y tres (3) Líneas de Defensa. A continuación, se detallan las responsabilidades asignadas a cada una de estas líneas:

LÍNEA ESTRATEGICA Define el marco general para la gestión del riesgo y el control, supervisa su cumplimiento.	
RESPONSABLE	**RESPONSABILIDAD**
Alta Dirección Comité Institucional de Coordinación de Control Interno	• Asumir la responsabilidad primaria del Sistema de Control Interno, de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo. • Definir e impartir lineamientos relacionados con el marco general para la administración de los riesgos. • Aprobar la Política de Administración del Riesgo. • Realizar recomendaciones orientadas a la mejora y actualización de la Política de Administración del Riesgo. • Supervisar el cumplimiento de la Política de Administración del Riesgo. • Revisar los resultados del monitoreo y seguimiento de los riesgos, generar alertas y recomendaciones cuando sea necesario. • Identificar conflictos de interés que puedan generar riesgos de corrupción. • Revisar y aprobar las matrices de riesgos.

PRIMERA LÍNEA DE DEFENSA Desarrolla e implementa procesos de control y de gestión de riesgos a través de su identificación, análisis, monitoreo y acciones de mejora.	
RESPONSABLE	**RESPONSABILIDAD**
Líderes de Proceso Director de Proyectos y Formuladores de Proyectos	• Promover la administración de los riesgos en los equipos internos de trabajo. • Identificar, analizar, valorar y actualizar, cuando sea necesario, los riesgos del proceso o proyecto bajo su responsabilidad. • Diseñar, aplicar y monitorear los controles de manera directa, para mitigar los riesgos identificados y proponer mejoras para su gestión.

Integrantes de Equipo Operativo del Sistema de Gestión y Desempeño	• Documentar la identificación del riesgo, análisis de causas, acciones de control establecidas, valoración y gestión de los riesgos en la matriz de riesgos. • Orientar el desarrollo e implementación de las políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la Entidad. • Verificar directamente el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y que su documentación se encuentre soportada en los procedimientos de los procesos. • Efectuar el monitoreo a los mapas de riesgo a su cargo, analizar los resultados del seguimiento y formular, establecer o adoptar las acciones correspondientes ante cualquier desviación. • Reportar al GIT de Planeación y al GIT de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información, los avances y soportes (evidencias) de la gestión de los riesgos dentro de los plazos establecidos. • Comunicar al equipo de trabajo los resultados de la gestión del riesgo. • Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Establecer, documentar y gestionar la implementación de planes de mejoramiento para los riesgos que se identifique su materialización.
Servidores públicos y colaboradores	• Participar en el diseño de los controles bajo su responsabilidad. • Ejecutar los controles conforme han sido diseñados.

	• Generar con oportunidad las alertas correspondientes, ante la posible materialización de los riesgos. • Informar al superior jerárquico o supervisor de contrato sobre los riesgos materializados o desviaciones en la aplicación de los controles. • Proponer mejoras a los controles existentes para optimizar su efectividad.

SEGUNDA LÍNEA DE DEFENSA

Asegura[2] que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen conforme con lo establecido por las disposiciones legales y reglamentarias, así como por las políticas y procedimientos internos. Es responsable de monitorear la gestión de riesgos y controles ejecutados por la primera línea de defensa, acompañando a los procesos en la administración de riesgos y en la consolidación de los mapas de riesgos.

RESPONSABLE	**RESPONSABILIDAD**
GIT de Planeación	• Asesorar a la línea estratégica en la formulación de la política y los lineamientos generales para la administración de riesgos.
GIT de Apoyo Informático, Oficial de Seguridad y Privacidad de la Información articulado con el GIT de Planeación	• Actualizar la política de administración de riesgos, especialmente en lo relacionado con los riesgos de seguridad de la información y seguridad digital.
El GIT de Planeación y GIT	• Acompañar a los líderes de los procesos y sus equipos en identificación de los riesgos y

---

[2] Asociado a la garantía de que los procesos, actividades, operaciones y resultados de una entidad pública se realicen de acuerdo con las normas, políticas y planes establecidos. Esto implica la verificación y evaluación objetiva para asegurar la eficiencia, eficacia, transparencia y legalidad de la gestión.

de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información (según aplique)	controles para la gestión de riesgos y su mejora continua. • Realizar seguimiento periódico a todos los riesgos, permitiendo que se generen recomendaciones y ajustes necesarios a los mapas de riesgos. • Realizar seguimiento y evaluar los controles aplicados por la primera línea de defensa. • Presentar los mapas de riesgos consolidados para la socialización y aprobación al Comité Institucional de Coordinación de Control Interno.
GIT Logístico de Capacitación y Prensa	• Revisar que la información interna y externa de la Entidad, cumpla con las disposiciones legales, reglamentarias y demás lineamientos impartidos por la Presidencia de la República en materia de comunicación pública. • Realizar seguimiento a los controles aplicados por la primera línea de defensa en materia de comunicaciones, capacitación y prensa.
Secretaría General en articulación con el Coordinador del GIT de Servicios Generales, Administrativos y Financieros	• Consolidar los avances del Plan Anual de Adquisiciones y generar alertas ante posibles retrasos o incumplimientos y reportar en el Comité de Coordinación de Control Interno para definir acciones de mejora. • Realizar seguimiento a los controles aplicados por la primera línea de defensa en materia de contratación.
Secretaría General en articulación con el Coordinador del GIT de Talento Humano y Prestaciones Sociales	• Consolidar los avances sobre el Plan Institucional de Capacitación (PIC), Bienestar, Incentivos y temas de convivencia laboral, y generar alertas sobre la ejecución de recursos y reportar en el Comité de Coordinación de Control Interno para definir acciones de mejora. • Realizar seguimiento a los controles aplicados por la primera línea de defensa en materia de gestión del talento humano.

Coordinador del GIT de Jurídica	• Verificar la gestión judicial y generar alertas sobre los procesos que se encuentran abiertos y sus cuantías, y reportar en las instancias correspondientes (Comité de Conciliación y el Comité Institucional de Coordinación de Control Interno) para definir acciones de mejora. • Realizar seguimiento a los controles aplicados por la primera línea de defensa en materia de gestión jurídica.

TERCERA LÍNEA DE DEFENSA

Garantiza la efectividad del Sistema de Control Interno. A diferencia de las primeras dos líneas, que están enfocadas en la gestión operativa y el cumplimiento, la tercera línea proporciona una evaluación independiente y objetiva, identifica áreas de mejora y propone acciones correctivas. Se encarga de realizar la medición de los avances de las acciones de respuesta y evaluación de la política.

RESPONSABLE	**RESPONSABILIDAD**
Grupo Interno de Trabajo de Control Interno	• Asesorar proactiva y estratégicamente a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. • Asesorar a la primera línea en las metodologías para la identificación y administración de los riesgos y el diseño de controles, en coordinación con la segunda línea de defensa (GIT de Planeación). • Recomendar mejoras a la política para la administración del riesgo. • Evaluar la efectividad de los controles para evitar la materialización de riesgos. • Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.

	• Proponer esquemas de asesoría y acompañamiento articuladas con el GIT de Planeación, en el marco del Plan Anual de Auditorías y Seguimientos. • Articularse con la GIT de Planeación y la GIT de Apoyo Informático, para compartir información y análisis de contraste que permita monitorear la exposición de la Entidad al riesgo y realizar recomendaciones de forma integral con alcance preventivo. • Comunicar al Comité Institucional de Coordinación de Control Interno los posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías.

6. METODOLOGÍA APLICADA

La UAE Contaduría General de la Nación adopta para la administración del riesgo la metodología establecida por el Departamento Administrativo de la Función Pública (DAFP) en el documento denominado: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" – Versión 6 y en la Metodología General Ajustada (MGA WEB). Estos documentos, emitidos por entidades del orden nacional, proporcionan los lineamientos necesarios para una gestión estructurada, coherente de los riesgos, alineada con los objetivos institucionales.

En concordancia con lo anterior, el enfoque aplicado es cíclico y participativo, y permite identificar, analizar, valorar y gestionar los riesgos de forma continua. A través de este proceso, la Entidad fortalece la toma de decisiones, anticipa situaciones críticas y promueve una cultura de prevención y mejora permanente.

A continuación, se presentan las etapas que componen este ciclo, junto con una breve descripción de cada una.

Fuente: Elaboración propia GIT de Planeación

1. Política de Administración del Riesgo: expresa el compromiso de la alta dirección frente a la gestión de riesgos, estableciendo los principios y lineamientos que orientan las acciones institucionales para anticipar, mitigar y responder adecuadamente ante posibles amenazas.

2. Identificación de Riesgos: consiste en reconocer los eventos o situaciones que podrían afectar el cumplimiento de los objetivos institucionales. Se analizan tanto factores internos como externos, considerando el contexto estratégico, los procesos operativos y los proyectos en ejecución

3. Análisis y valoración de riesgos: busca comprender la naturaleza de cada riesgo identificado. Para ello, se evalúa su probabilidad de ocurrencia y su impacto potencial, se clasifican según su severidad (riesgo inherente y residual) y se identifican los controles existentes.

4. Tratamiento de riesgos: implica definir las acciones que se deben implementar para reducir, eliminar o aceptar los riesgos residuales. Esta etapa orienta la toma de decisiones sobre el manejo adecuado de los riesgos priorizados.

5. Monitoreo y revisión: se realiza de forma continua por las tres líneas de defensa, con énfasis en las responsabilidades de la primera y segunda línea. Permite verificar si los riesgos están siendo gestionados conforme a lo planeado y si los controles aplicados son eficaces.

Las siguientes etapas se ejecutan de manera transversal junto con las indicadas anteriormente.

6. Evaluación: esta actividad se desarrolla bajo las líneas de defensa, sin embargo, la evaluación se encuentra a cargo principalmente de la tercera línea de defensa, esta etapa garantiza una visión independiente sobre la efectividad del sistema de gestión de riesgos y permite recomendar ajustes o mejoras cuando sea necesario.

7. Comunicación y Consulta: es un proceso transversal que asegura que la información relacionada con los riesgos fluya de manera oportuna y comprensible. Favorece la participación activa

de todos los actores y fortalece la cultura de gestión del riesgo dentro de la entidad.

7. CONTEXTO

Para la identificación de los riesgos que podrían impactar su desempeño, la Entidad realizó en el marco de su planeación estratégica, un análisis de su entorno estratégico, considerando factores internos y externos que podrían influir en la consecución de los objetivos institucionales.

Contexto externo

En cuanto al contexto externo, la Entidad identificó los siguientes factores:

- **Competitivos:** se evaluaron aspectos como la imagen corporativa, las alianzas con instituciones públicas y privadas para ejecutar programas y proyectos, el apoyo de la cooperación internacional, así como la participación en eventos académicos y profesionales. Asimismo, se tuvo en cuenta la cultura contable, el conocimiento institucional y el posicionamiento de la CGN.
- **Sociales:** se destacó la inestabilidad e informalidad laboral en el país, la disminución de la oferta de personal calificado, la falta de información requerida y las situaciones de orden público que podrían afectar el cumplimiento de las funciones de la entidad.
- **Económicos: s**e identificó el recorte presupuestal como un factor de riesgo que podría limitar la capacidad operativa de la Entidad.
- **Tecnológicos:** se consideraron tanto oportunidades como riesgos derivados de la automatización de procesos, los posibles ciberataques a los sistemas de información, los cambios tecnológicos, la escasez de proveedores de tecnología y la disponibilidad presupuestal para estos recursos.

- **Políticos:** se analizó la credibilidad en las instituciones del Estado, los cambios en la política general que afectan a la entidad, la estabilidad política, y las normas que podrían afectar el cumplimiento de los objetivos de la entidad.
- **Geográficos:** se evaluó el nivel de desarrollo económico y social de las regiones que rodean la entidad**.**

Contexto interno

En relación con el contexto interno, la Entidad consideró los siguientes aspectos clave:

- **Capacidad Directiva:** se valoró la imagen que proyecta la alta dirección, la claridad en los planes estratégicos y operativos, la orientación institucional hacia el cumplimiento de la misión, así como la estructura organizacional y los mecanismos de toma de decisiones y control directivo sobre la operación.
- **Capacidad del Talento Humano:** se identificaron factores como la rotación de personal, la habilidad para atraer y retener talento calificado, el nivel de competencias del personal, la motivación y el sentido de pertenencia de los servidores públicos, además de los programas de formación y desarrollo profesional.
- **Capacidad Tecnológica:** se evaluó la capacidad de innovación de la entidad, la resistencia al cambio, la actualización e integración de sistemas, así como la seguridad de las plataformas tecnológicas y la competencia técnica de la entidad para ejecutar sus procesos.
- **Capacidad Competitiva**: se analizó la cultura contable que genera la CGN, el índice de desempeño, el impacto de los bienes y servicios entregados por la entidad a sus grupos de interés, la capacidad para ejecutar proyectos, el conocimiento oportuno y capacidad de atención a las quejas y reclamos de los grupos de interés, la eficiencia de los servicios

que presta o suministra la entidad, y la obtención de certificaciones en normas de calidad.

- **Capacidad Financiera**: se revisaron los niveles de eficiencia y eficacia en la ejecución presupuestal, el déficit o superávit acumulado o proyectado, así como la estructura de ingresos y gastos de la Entidad.

8. NIVELES PARA CALIFICAR LA PROBABILIDAD

A continuación, se presentan los criterios de probabilidad que aplican para los riesgos de gestión, fiscal y de seguridad de la información y seguridad digital.

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo. Está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. En ese sentido, la probabilidad se calcula considerando la frecuencia con la que el proceso o actividad se ve expuesto al riesgo durante un periodo de un (1) año. De esta manera, se mide el número de veces que se presenta la oportunidad de materialización del riesgo en dicho periodo.

A continuación, se presentan los criterios de probabilidad aplicables a los riesgos de corrupción, los cuales se clasifican según la frecuencia y la exposición al riesgo de corrupción dentro de la Entidad:

	Frecuencia de la Actividad	**Probabilidad**
Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de 1 vez al año

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

A continuación, se presentan los criterios de probabilidad que aplica para los riesgos de proyectos.

	Valor de la probabilidad
Raro	1
Improbable	2
Moderado	3
Probable	4
Casi seguro	5

Fuente: Metodología General Ajustada para Proyectos de Inversión - DNP

9. NIVELES PARA CALIFICAR EL IMPACTO

En los riesgos de gestión y fiscal los niveles para calificar el impacto son los siguientes:

Nivel	Afectación económica	Afectación Operacional	Reputacional
Leve 20%	Afectación menor o igual a 20 SMLV	Impacta la ejecución o continuidad de una tarea	El riesgo afecta la imagen de algún área de la entidad en el ámbito interno
Menor 40%	Mayor a 20 y menor o igual a 120 SMLV	Impacta la ejecución o continuidad de una actividad	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Mayor a 120 y menor o igual a 500 SMLV	Impacta la ejecución o continuidad de un procedimiento, manual o protocolo	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Mayor a 500 y menor o igual a 1300 SMLV	Impacta la ejecución o continuidad de un proceso o subproceso	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 1300 SMLV	Impacta la ejecución o continuidad de un macroproceso, varios procesos o proyectos de la Entidad	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6 y construcción propia de la CGN

En los riesgos de corrupción, los niveles para calificar el impacto, de acuerdo con lo establecido por la Secretaría de Transparencia de la Presidencia de la República, son los siguientes:

Nivel	Descriptor	Consecuencias
Moderado	Respuesta afirmativa de una a cinco preguntas	Genera medianas consecuencias para la entidad
Mayor	Respuesta afirmativa de seis a once preguntas	Genera altas consecuencias para la entidad
Catastrófico	Respuesta afirmativa de doce a diecinueve preguntas	Genera desastrosas consecuencias para la entidad

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

En línea con lo anterior, las siguientes preguntas están diseñadas para evaluar las posibles repercusiones en distintos niveles de la Entidad y el entorno en el que opera; con el fin de facilitar la valoración del impacto para los riesgos de corrupción, se detallan a continuación:

Pregunta		Respuesta	
No.	**¿Si el riesgo de corrupción o fraude se materializa,...?**:	SI	NO
1	¿Afecta al grupo de funcionarios del proceso?		
2	¿Afecta el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afecta el cumplimiento de la misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Genera pérdida de confianza de la entidad, afectando su reputación?		
6	¿Genera pérdida de recursos económicos?		

Pregunta		**Respuesta**	
7	¿Afecta la generación de los productos o la prestación de los servicios?		
8	¿Podría causar un detrimento de calidad de vida de la comunidad por la pérdida de bienes, servicios o recursos públicos?		
9	¿Genera pérdida de la información de la entidad?		
10	¿Genera intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Da lugar a procesos sancionatorios?		
12	¿Da lugar a procesos disciplinarios?		
13	¿Da lugar a procesos fiscales?		
14	¿Da lugar a procesos penales?		
15	¿Genera pérdida de credibilidad del sector?		
16	¿Ocasiona lesiones físicas o pérdidas de vidas humanas?		
17	¿Afecta la imagen regional?		
18	¿Afecta la imagen nacional?		
19	¿Afecta la imagen internacional?		

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

En los riesgos de seguridad de la información y seguridad digital, los niveles para calificar el impacto son:

Nivel	**Valor del impacto**	**Consecuencias Cualitativas**
Leve	1	• Sin afectación de la integridad. • Sin afectación de la disponibilidad. • Sin afectación de la confidencialidad.
Menor	2	• Afectación leve de la integridad. • Afectación leve de la disponibilidad. • Afectaciones leves de la confidencialidad.

Nivel	Valor del impacto	Consecuencias Cualitativas
Moderado	3	• Afectación moderada de la integridad por interés de empleados y terceros. • Afectación moderada de la disponibilidad por interés de empleados y terceros. • Afectación moderada de la confidencialidad por interés de empleados y terceros.
Mayor	4	• Afectación grave de la integridad por interés de los empleados y terceros. • Afectación grave de la integridad debido al interés de los empleados y terceros. • Afectación grave de la confidencialidad debido al interés de los empleados y terceros.
Catastrófico	5	• Afectación muy grave de la integridad por interés de los empleados y terceros. • Afectación muy grave de la disponibilidad por interés de los empleados y terceros. • Afectación muy grave de la confidencialidad por interés de los empleados y terceros.

Fuente: Elaboración propia

En los riesgos de seguridad de la información y seguridad digital, los niveles para calificar el impacto son:

Impacto	Descriptor
Moderado	Genera medianas consecuencias sobre la entidad.
Mayor	Genera altas consecuencias sobre la entidad.
Catastrófico	Genera consecuencias muy graves para la entidad.

Fuente: Elaboración propia

En los riesgos de proyectos, los niveles para calificar el impacto son:

Impacto	Valor del impacto
Insignificante	1
Menor	2
Moderado	3
Mayor	4
Catastrófico	5

Fuente: Metodología General Ajustada para Proyectos de Inversión – DNP

10. NIVELES DE ACEPTACIÓN DEL RIESGO

Para el caso de los riesgos de gestión, fiscales, proyectos y de seguridad de la información se consideran ACEPTABLES aquellos ubicados en nivel de riesgo bajo.

Los riesgos de corrupción **NO TIENEN** nivel de aceptación.

11. ESTRATEGIAS PARA COMBATIR EL RIESGO

Las estrategias para la mitigación de riesgos, incluyendo los riesgos de corrupción, son establecidas por la primera línea de defensa. En la CGN, estas opciones están orientadas a la toma de decisiones que permitan gestionar eficazmente los riesgos, a través de las siguientes acciones:

- **Reducir el riesgo:** El riesgo debe ser gestionado mediante la implementación de controles que permitan reevaluar el riesgo residual como aceptable para la entidad. Estos controles suelen reducir la probabilidad y/o el impacto del riesgo, minimizando sus efectos.
    - Transferir el riesgo: Tras un análisis, puede considerarse que la mejor estrategia es externalizar el proceso o transferir el riesgo

mediante pólizas. En este caso, la responsabilidad económica recae sobre un tercero, aunque la responsabilidad reputacional sigue siendo de la entidad.

  - Mitigar el riesgo: Tras evaluar los niveles de riesgo, se implementan acciones para reducir su nivel. Esto no necesariamente implica añadir nuevos controles, sino realizar ajustes que disminuyan los efectos del riesgo.

- **Aceptar el riesgo:** Cuando el nivel de riesgo cumple con los criterios establecidos de aceptación, no se implementan controles adicionales y el riesgo es considerado aceptable. Esta estrategia aplica principalmente a los riesgos inherentes en la zona de bajo riesgo, aunque no se permite aceptar ningún riesgo relacionado con la corrupción. (Ningún riesgo de corrupción podrá ser aceptado)
- **Evitar el riesgo:** Si los escenarios de riesgo identificados se consideran demasiado extremos o inaceptables, se puede optar por evitar el riesgo, eliminando actividades o procesos que lo generen.

Para asegurar el logro de los objetivos institucionales, las actividades de control están orientadas tanto a prevenir como a detectar la materialización de los riesgos. La efectividad de estas actividades depende de la medida en que se logren los objetivos estratégicos y operativos de la Entidad.

Es responsabilidad de la primera línea de defensa establecer las actividades de control, lo que implica equilibrar los costos y los esfuerzos necesarios para su implementación, en relación con los beneficios finales esperados. Por lo tanto, para la implementación de acciones y controles, es esencial considerar aspectos como la viabilidad jurídica, técnica, institucional, financiera y económica, así como realizar un análisis de costo-beneficio.

De acuerdo con lo anterior, se presentan a continuación las opciones de tratamiento para cada nivel de riesgo:

Nivel de Exposición del Riesgo	Opción de Tratamiento	Detalle del Tratamiento
ZONA DE RIESGO EXTREMO	Reducir: Mitigar	Se deberán implementar inmediatamente las acciones que conlleven a reducir el riesgo. Las acciones preventivas tomadas deberán llevar a la implementación de nuevos controles que prevengan la materialización del riesgo y a mitigar el impacto.
ZONA DE RIESGO ALTO	Reducir: Mitigar o Transferir	Se deberán implementar acciones que conlleven a mitigar o transferir el riesgo. Se deberán implementar acciones preventivas que conlleven a mejorar o documentar los controles existentes.
ZONA DE RIESGO MODERADO	Reducir: Mitigar o Transferir	Se deberán implementar acciones que conlleven a reducir el riesgo. Se deberán implementar acciones preventivas que conlleven a fortalecer los controles existentes.
ZONA DE RIESGO BAJO	Aceptar	Se debe realizar seguimiento a los riesgos con el fin de verificar su impacto, probabilidad y la valoración de los controles.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

12. MATERIALIZACIÓN DE RIESGOS

La siguiente tabla presenta las acciones a seguir por parte de para cada una de las líneas de defensa en caso de que se materialice un riesgo.

	Primera Línea de Defensa	**Segunda Línea de Defensa**	**Tercera Línea de Defensa**	**Línea Estratégica**
Acciones generales frente a la materialización de riesgos	1. Realizar el análisis de causas, estableciendo los impactos generados en el proceso y determinando las acciones correctivas, preventivas, y de mejora. Nota: En caso de considerarlo necesario, solicitar el acompañamiento metodológico de la	1. El GIT de Planeación o el GIT de Apoyo Informático con apoyo del Oficial de Seguridad y Privacidad de la Información (según aplique) deben revisar el análisis de causas y las acciones correctivas de los Planes de Mejoramiento planteados por la primera línea de defensa, y realizar las recomendaciones que permitan asegurar	1. Evaluar la efectividad de las acciones implementadas por la primera línea de defensa. 2. Evaluar la efectividad de los controles planteados por la primera línea de defensa sean efectivos, le apunten al riesgo y estén	1. El Comité Institucional de Coordinación de Control Interno - CICCI deberá realizar el monitoreo y seguimiento correspondiente del impacto generado, con el fin de tomar las acciones correspondientes que permitan asegurar el cumplimiento de los objetivos y metas institucionales. Lo

	Primera Línea de Defensa	Segunda Línea de Defensa	Tercera Línea de Defensa	Línea Estratégica
	segunda línea de defensa. 2. Informar al GIT de Planeación como segunda línea de defensa, sobre la materialización del riesgo. 3. Remitir al GIT de Planeación para su revisión, el Plan de Mejoramiento que incluya: análisis de causas, la evaluación de los impactos de la materialización del riesgo y las acciones correctivas propuestas por el proceso o proyecto, para	que los controles estén bien diseñados. 2. El GIT de Planeación o el GIT de Apoyo Informático con apoyo del Oficial de Seguridad y Privacidad de la Información (según aplique) deben presentar el Plan de Mejoramiento de la materialización del riesgo en el CICCI, el cual debe incluir como mínimo: la descripción del hallazgo, el tipo de hallazgo u observación, análisis de causa, descripción de la acción a realizar, el producto esperado, fecha iniciación de la acción, fecha	funcionando en forma adecuada. 3. Verificar y evaluar la efectividad de las acciones implementadas en el Plan de Mejoramiento.	anterior a partir de los informes presentados por la segunda y tercera línea de defensa. 2. Adoptar las acciones que considere pertinentes, las cuales serán de obligatorio cumplimiento para cada una de las líneas de defensa. 3. Impartir lineamientos orientados a prevenir que el riesgo se vuelva a materializar.

	Primera Línea de Defensa	**Segunda Línea de Defensa**	**Tercera Línea de Defensa**	**Línea Estratégica**
	mitigar el impacto y evitar que el riesgo se vuelva a materializar. 4. Atender las recomendaciones realizadas por la segunda y tercera línea, para la identificación de riesgos. 5. Revisar y ajustar los controles existentes. De ser necesario, establecer nuevos controles asociados al riesgo materializado, teniendo en cuenta el Plan de Mejoramiento definido.	finalización de la acción, responsable de la acción, seguimiento y el estado. 3. Realizar seguimiento a las acciones de monitoreo implementadas por la primera línea de defensa. 4. Verificar el cumplimiento de las acciones planteadas en el Plan de Mejoramiento y se actualizó el Mapa de Riesgos correspondiente.		

	Primera Línea de Defensa	Segunda Línea de Defensa	Tercera Línea de Defensa	Línea Estratégica
	6. Revisar y actualizar el Mapa de Riesgos correspondiente, en particular las causas, riesgos y controles, estableciendo acciones preventivas y de mejora. 7. Dar cumplimiento estricto al Plan de Mejoramiento propuesto.			
Acciones específicas respecto a los riesgos de corrupción frente	1. Revisar las causas asociadas a la materialización del Riesgo de Corrupción y adoptar las	1. El GIT de Planeación debe revisar el Mapa de Riesgos de corrupción, en particular, las causas, riesgos y controles.	1. Verificar y evaluar la efectividad de las acciones planteadas en el	1. Una vez surtido el conducto regular establecido por la Entidad y dependiendo del alcance

	Primera Línea de Defensa	Segunda Línea de Defensa	Tercera Línea de Defensa	Línea Estratégica
a su materialización	medidas correspondientes para evitar el mayor impacto. 2. Establecer nuevos controles que permitan prevenir que se vuelva a materializar. 3. Solicitar el acompañamiento del GIT de Jurídica para determinar la pertinencia de adelantar las indagaciones correspondientes.	2. El GIT de Planeación debe llevar a cabo un monitoreo de los procesos que han materializado riesgos. 3. El GIT de Planeación debe consolidar y publicar en la página web de la CGN, el Mapa de Riesgos de corrupción actualizado.	Plan de Mejoramiento. 2. Verificar y evaluar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción. 3. Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.	(normatividad asociada al hecho de corrupción materializado), analiza y determina la aplicabilidad del proceso disciplinario e informa a la instancia respectiva. 2. Informar a las autoridades correspondientes de la ocurrencia de un hecho de corrupción.
Acciones específicas respecto a los riesgos de seguridad de la	1. En caso de materialización de un riesgo de seguridad digital o ciberseguridad, se	1. El GIT de Apoyo Informático con apoyo del Oficial de Seguridad y Privacidad de la	1. Verificar y evaluar el diseño e idoneidad de los controles y si son adecuados para	No aplica

	Primera Línea de Defensa	**Segunda Línea de Defensa**	**Tercera Línea de Defensa**	**Línea Estratégica**
información, seguridad digital y ciberseguridad frente a su materialización	debe informar, adicionalmente, al GIT de Apoyo Informático y al Oficial de Seguridad y Privacidad de la Información de la CGN. 2. En la elaboración de los controles para mitigar o tratar el riesgo, se debe tener en cuenta lo establecido en "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se	Información de la CGN, debe supervisar y acompañar el proceso de implementación de los Planes de Mejoramiento, verificando que la primera línea de defensa ejecute las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado. 2. El GIT de Apoyo Informático con apoyo del Oficial de Seguridad y Privacidad de la Información debe efectuar la evaluación	prevenir o mitigar los riesgos. 2. Considerar la pertinencia de priorizar en el Plan Anual de Auditorías y Seguimientos la evaluación a la efectividad del Plan de Contingencia y Tratamiento de Incidentes de Seguridad de la Información, Seguridad Digital y Ciberseguridad. 3. Emitir recomendaciones orientadas a	

	Primera Línea de Defensa	**Segunda Línea de Defensa**	**Tercera Línea de Defensa**	**Línea Estratégica**
	ajusten al análisis de riesgos. 3. Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información, seguridad digital y ciberseguridad que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar tanto en el Plan de Mejoramiento como en el registro de los incidentes de	de los Planes de Mejoramiento, realizar nuevamente la valoración de los riesgos de seguridad digital y ciberseguridad para verificar su efectividad, y realizar la actualización de los Mapas de Riesgo de Seguridad de la información, digital y ciberseguridad. 3. El GIT de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información debe actualizar el registro de los incidentes de seguridad digital y ciberseguridad que se hayan materializado,	fortalecer los controles de seguridad digital y minimizar vulnerabilidades en los sistemas de información.	

	Primera Línea de Defensa	**Segunda Línea de Defensa**	**Tercera Línea de Defensa**	**Línea Estratégica**
	seguridad digital y ciberseguridad. 4. Realizar los correctivos necesarios frente a los usuarios e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existentes, documentar en el Plan de Mejoramiento Institucional y actualizar el Mapa de Riesgos de Seguridad Digital y Ciberseguridad.	con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar, según lo indicado en los lineamientos para la gestión del riesgo de seguridad digital y ciberseguridad. 4. El GIT de Apoyo Informático junto con el Oficial de Seguridad y Privacidad de la Información debe garantizar la capacitación continua a los colaboradores sobre seguridad de la información, digital y ciberseguridad, sensibilizando el		

	Primera Línea de Defensa	**Segunda Línea de Defensa**	**Tercera Línea de Defensa**	**Línea Estratégica**
	5. Implementar buenas prácticas de seguridad digital, tales como el uso de contraseñas seguras, el manejo adecuado de la información confidencial y la protección contra ataques de ingeniería social.	manejo seguro de la información y la prevención de ataques cibernéticos.		
Acciones específicas respecto a los riesgos fiscales frente a su materialización	1. Realizar los correctivos necesarios e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los	1. El GIT de Planeación debe llevar a cabo un monitoreo de los procesos que han materializado riesgos. 2. Presentar a la Línea Estratégica un reporte relacionado con las observaciones detectadas en el	1. Verificar y evaluar la efectividad de las acciones planteadas en el Plan de Mejoramiento. 2. Verificar y evaluar el diseño y efectividad de	1. Analizar y determinar la pertinencia de compulsar la información a la instancia correspondiente interna o externa, con el fin de que se indaguen las circunstancias que dieron lugar a la

	Primera Línea de Defensa	**Segunda Línea de Defensa**	**Tercera Línea de Defensa**	**Línea Estratégica**
	controles existentes, documentar en el Plan de Mejoramiento Institucional y actualizar el Mapa de Riesgos. 2. Solicitar el acompañamiento del GIT de Jurídica para analizar los hechos constitutivos de la materialización del riesgo fiscal y adoptar las acciones correspondientes. 3. Presentar a la segunda línea de defensa un informe detallado	monitoreo del riesgo materializado.	los controles, si se encuentran orientados a mitigar los riesgos fiscales y presentar a la línea estratégica las recomendaciones que se consideren pertinentes. 3. Verificar si se tomaron las acciones y se actualizó el mapa de riesgos en lo relacionado con los riesgos fiscales.	materialización del riesgo fiscal.

	Primera Línea de Defensa	Segunda Línea de Defensa	Tercera Línea de Defensa	Línea Estratégica
	sobre los hechos y causas constitutivas de la materialización del riesgo fiscal y las acciones y decisiones adoptadas con el acompañamiento del GIT de Jurídica			

13. MONITOREO Y REVISIÓN

Primera línea de defensa:
La primera línea de defensa (líderes de los procesos) será responsable de elaborar la matriz de riesgos, para lo cual deberá identificar los riesgos, analizar las causas y establecer acciones que directamente relacionadas a mitigar las causas y los riesgos establecidos de manera coherente, realizar el monitoreo y la revisión periódica de la aplicación de los controles establecidos para la gestión de riesgos con una periodicidad mínimo trimestral.

Este ejercicio debe concretarse en un informe que incluya:
- El seguimiento a los riesgos identificados.
- La aplicación de los controles.
- Avance en la implementación de los planes de acción.
- Registro de la materialización de riesgos.
- Reporte de novedades relevantes relacionadas con la gestión del riesgo.

El informe deberá remitirse al GIT de Planeación y, en el caso de riesgos asociados a seguridad de la información, se deberá remitir al GIT de Apoyo Informático y al Oficial de Seguridad y Privacidad de la Información, dentro de los primeros diez (10) días calendario del mes siguiente al cierre de cada trimestre.

Lo anterior, teniendo en cuenta los siguientes cortes trimestrales:
- Primer trimestre: 31 de marzo
- Segundo trimestre: 30 de junio
- Tercer trimestre: 30 de septiembre
- Cuarto trimestre: 31 de diciembre

Segunda línea de defensa:

El GIT de Planeación y el GIT de Apoyo Informático junto al Oficial de Seguridad y Privacidad de la Información (para riesgos de seguridad de la información) realizarán el seguimiento al monitoreo reportado por la primera línea de defensa mediante el análisis de una muestra aleatoria de procesos. A partir de esta revisión, emitirán observaciones, alertas y recomendaciones, dentro del mes siguiente al respectivo corte.

Nota: En atención a lo anterior, el primer monitoreo efectuado por la segunda línea de defensa se realizará con corte al 30 de septiembre de 2025.

14. EVALUACIÓN

El GIT de Control Interno (Tercera Línea de Defensa) realizará la evaluación de los riesgos de la Entidad en el marco de las auditorías internas o seguimientos incluidos en el Plan de Auditoría y Seguimiento aprobado por el Comité Institucional de Coordinación de Control Interno para cada vigencia.

La evaluación a los riesgos de corrupción tendrá una periodicidad cuatrimestral; el informe de los resultados se realizará y se publicará en la página web de la Entidad en las siguientes fechas:

- Primer seguimiento: con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

Con relación a los riesgos de gestión, fiscal, de seguridad de la información y seguridad digital y proyectos, el GIT de Control Interno podrá incluir una muestra aleatoria dentro de la evaluación cuatrimestral a los riesgos de corrupción.

En todo caso, dichos riesgos deberán ser evaluados mínimo una (1) vez al año, para lo cual, el GIT de Control Interno dentro de su independencia, podrá establecer la metodología que considere pertinente, con el fin de garantizar la evaluación de la mayor cantidad de riesgos de gestión, fiscal, de seguridad de la información y seguridad digital y proyectos.

Adicionalmente, en el desarrollo del Plan Anual de Auditorías y Seguimientos, el GIT de Control Interno evaluará los riesgos asociados a los procesos, procedimientos, proyectos y políticas objeto de las auditorías o evaluaciones e informes de ley.

15. DIVULGACIÓN

La Política de Administración del Riesgo, los Mapas de Riesgos: institucional, gestión, fiscal, corrupción, seguridad de la Información - seguridad digital y de proyectos, se divulgarán a través de la página web de la Contaduría General de la Nación a fin de que todas las partes interesadas se informen de la gestión de riesgos realizada por los procesos.

16. CAPACITACIÓN

La administración del riesgo es un eje fundamental para el cumplimiento de los objetivos institucionales. Por tanto, se deberá garantizar, como mínimo, la realización de una capacitación anual (ya sea de carácter interno o externo) dirigida a los servidores públicos. Esta formación permitirá fortalecer sus competencias y asegurar una administración del riesgo coherente, eficaz y alineada con los procesos de la entidad