

**INFORME EJECUTIVO DE REVISIÓN Y SEGUIMIENTO AL
MONITOREO DE LOS RIESGOS DE GESTIÓN, FISCALES,
CORRUPCIÓN, SEGURIDAD DE LA INFORMACIÓN Y
PROYECTOS DE INVERSIÓN**

TERCER TRIMESTRE DE 2025

**SEGUNDA LÍNEA DE DEFENSA
GIT DE PLANEACIÓN**

Tabla de contenido

1. INTRODUCCIÓN.....	3
2. OBJETIVO	3
3. ALCANCE.....	3
4. METODOLOGÍA.....	4
5. ACTUALIZACIÓN DE RIESGOS DE LA CGN.....	5
6. RESULTADOS DE LA REVISIÓN AL MONITOREO DE LA PRIMERA LÍNEA DE DEFENSA.....	5
6.1. Observaciones y recomendaciones de la segunda línea de defensa para los riesgos de gestión, fiscales y corrupción	6
6.2. Observaciones y recomendaciones de la segunda línea de defensa para los riesgos de seguridad de la información y seguridad digital.....	7
6.3. Observaciones y recomendaciones de la segunda línea de defensa para los riesgos en proyectos de inversión.....	7
7. CONCLUSIONES Y RECOMENDACIONES	7
ANEXO 1	9

1. INTRODUCCIÓN

En línea con la **Política de Administración del Riesgo de la CGN**, el presente informe muestra los resultados de la revisión del monitoreo de los riesgos de la Entidad correspondientes al tercer trimestre de 2025, realizado por la **segunda línea de defensa**.

El seguimiento y revisión de los riesgos vigentes busca **disminuir la probabilidad de ocurrencia y el impacto de los eventos inesperados** que puedan afectar el cumplimiento de la misión, visión, objetivos institucionales, objetivos de los procesos y, sobre todo, la calidad de los productos y servicios prestados por la CGN.

En este documento se presentan la **metodología utilizada**, los **resultados obtenidos**, así como las **conclusiones y recomendaciones** derivadas del ejercicio de monitoreo.

2. OBJETIVO

Efectuar la **revisión del monitoreo de los riesgos vigentes en la CGN** con el propósito de asegurar el logro de los objetivos institucionales.

Se pretende socializar los resultados obtenidos a partir de la **Política de Administración del Riesgo vigente**, la **actualización de la matriz de riesgos** (gestión, fiscales, corrupción y seguridad de la información) **y el monitoreo** reportado por la primera línea de defensa.

Adicionalmente, se presentan las **conclusiones y recomendaciones** derivadas de la revisión realizada.

3. ALCANCE

La revisión corresponde al periodo comprendido entre **el 21 de agosto de 2025 y el 30 de septiembre de 2025¹** y abarca todos los procesos de la entidad en las siguientes tipologías de riesgo:

¹ El periodo esta alineado a la aprobación de las matrices de riesgos de gestión, fiscales y corrupción, y seguridad de la información y seguridad digital en el Comité de Coordinación Institucional de Control Interno efectuado el 21 de agosto de 2025.

- Gestión
- Fiscales y corrupción
- Seguridad de la información y seguridad digital

Para los Riesgos de todos los proyectos de inversión vigentes, la revisión corresponde al **tercer trimestre de 2025**

4. METODOLOGÍA

La revisión del monitoreo de riesgos se efectuó con base en las **matrices de riesgos vigentes durante el tercer trimestre de 2025 y aprobadas en el Comité Institucional de Coordinación de Control Interno el 21 de agosto de 2025**, y el seguimiento realizado por la **primera línea de defensa**, considerando:

- 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.

Según el numeral 13 de la **Política de Administración del Riesgo**, "el GIT de Planeación y el GIT de Apoyo Informático, junto al Oficial de Seguridad y Privacidad de la Información, realizarán el seguimiento al monitoreo reportado por la primera línea de defensa mediante el análisis de una **muestra aleatoria de procesos**".

Para esta revisión, se seleccionó la siguiente muestra:

- 7 riesgos de gestión
- 1 riesgo fiscal
- 7 riesgos de corrupción (total de riesgos de corrupción)
- 5 riesgos de proyectos
- 6 riesgos de seguridad de la información y seguridad digital

Para un mayor detalle, ver Anexo 1.

El primer monitoreo efectuado por la segunda línea de defensa se realizó con **corte al 30 de septiembre de 2025**.

5. ACTUALIZACIÓN DE RIESGOS DE LA CGN

Durante el **segundo y tercer trimestre de 2025**, la CGN realizó la actualización de la Política de Administración de Riesgos y de las matrices de riesgos en las tipologías de **gestión, fiscales, corrupción, seguridad de la información y seguridad digital**.

- Como resultado de la actualización de las matrices de riesgos, la CGN cuenta con 28 riesgos de gestión, 3 riesgos fiscales, 7 riesgos de corrupción, 18 de seguridad de la información y 21 riesgos de proyectos para un total de 77 riesgos identificados.
- Los riesgos de gestión y corrupción presentaron **una variación en su estructura con respecto a las matrices revisadas en el seguimiento del periodo anterior**, basada en la propia aplicación de la metodología y en el análisis interno de procesos, contexto, actividades, relacionamiento con partes interesadas y eventos relacionados con el riesgo.
- La actualización de riesgos de seguridad de la información se realizó con base en la **norma ISO/IEC 27001:2022 y el anexo A** de objetivos de control y controles de referencia.

Las matrices actualizadas fueron presentadas y aprobadas en el **Comité Institucional de Coordinación de Control Interno** el 21 de agosto de 2025.

6. RESULTADOS DE LA REVISIÓN AL MONITOREO DE LA PRIMERA LÍNEA DE DEFENSA

La revisión efectuada por la segunda línea de defensa al monitoreo de riesgos se presenta organizada en tres grupos de análisis.

En primer lugar, se aborda la revisión correspondiente a los riesgos clasificados en las tipologías de gestión, fiscales y corrupción.

En segundo lugar, se presentan los resultados del análisis de los riesgos de seguridad de la información y seguridad digital.

Finalmente, se incluye la revisión de los riesgos identificados en los proyectos de inversión de la Contaduría General de la Nación.

6.1. Observaciones y recomendaciones de la segunda línea de defensa para los riesgos de gestión, fiscales y corrupción

- Los procesos realizaron el monitoreo dentro de los **tiempos establecidos**.
- A nivel general, se recomienda fortalecer el monitoreo considerando:
 - a. Describir observaciones del periodo de monitoreo (aspectos de interés, decisiones tomadas).
 - b. Indicar novedades en cada riesgo, explicando su naturaleza y causa.
 - c. Para cada control, indicar si se aplicó, cómo se aplicó, si hubo desviaciones y evidencia asociada.
 - d. Para los casos en que los controles se encuentran en proceso de aplicación, se recomienda su reporte en el próximo monitoreo.
 - e. Incluir nombre de archivo o carpeta que respalde el control y cómo la evidencia soporta su aplicación de manera clara, explícita y conforme al diseño del control.
 - f. Presentar conclusiones por tipología y generales de los riesgos.
 - g. Para los procesos de **Centralización de la información – Riesgo 3, Consolidación de la información – Riesgo 3, Gestión Humana – Riesgo 5**, se recomienda que la evidencia de los controles muestre su aplicación por parte del responsable definido en el diseño.
 - h. Para el proceso de **Gestión Humana- Riesgo 3**, es importante aclarar que en el caso en que no se haya aplicado el control durante el periodo analizado, se precise de esa manera en el monitoreo.
 - i. Para el proceso de **Gestión humana – Riesgo 5**, se recomienda precisar la redacción de la evidencia de los dos controles para que se refleje tal y como se da en la operación.
 - j. Para el proceso de **Gestión TICs – Riesgos 2 y 3**, se recomienda que la evidencia corresponda únicamente al periodo analizado o que se describa en el informe de monitoreo el motivo por el cual se consideren evidencias fuera del periodo analizado.

6.2. Observaciones y recomendaciones de la segunda línea de defensa para los riesgos de seguridad de la información y seguridad digital

- Los procesos realizaron el monitoreo dentro de los **tiempos establecidos**.
- Se recomienda **continuar con el monitoreo**, considerando la verificación de controles por la segunda línea de defensa.
- Los **planes de acción** (tres en total) están en ejecución y culminarán en el último trimestre; se recomienda incluir su avance en el **próximo informe**.
- No se reportó **materialización de riesgos** durante el periodo.

6.3. Observaciones y recomendaciones de la segunda línea de defensa para los riesgos en proyectos de inversión

- Los procesos realizaron el monitoreo dentro de los **tiempos establecidos, excepto** el proyecto "*Fortalecimiento de la Generación de Información desde el Sistema de Información Misional de la CGN Bogotá*", cuyo reporte se entregó **5 días después** de la fecha establecida.
- En general, se recomienda fortalecer el monitoreo considerando:
 - a. Para cada medida de mitigación, indicar si se aplicó y cómo.
 - b. Incluir nombre de archivo o carpeta que respalte la ejecución de la medida y cómo la evidencia soporta su aplicación.
 - c. Presentar conclusiones del monitoreo de riesgos de proyectos.
- No se reportó **materialización de riesgos** durante el periodo.

7. CONCLUSIONES Y RECOMENDACIONES

- La **primera línea de defensa** realizó el reporte de los monitoreos dentro de los tiempos establecidos en la mayoría de los casos.
- Se identificó la necesidad de **fortalecer el informe del monitoreo**, incluyendo observaciones, novedades, aplicación de controles y evidencia.

- Los **planes de acción** se encuentran en curso o cumplidos según corresponda y se recomienda darles seguimiento en los próximos informes teniendo en cuenta sus fechas de vencimiento.
- No se reportó **materialización de riesgos** en ninguna de las tipologías durante el periodo de monitoreo.

Elaboró: Marcela Cárdenas / Martha Zornosa G
Revisó: Claudia Patricia Hernández

ANEXO 1

Tabla 1. Muestra de riesgos de gestión, fiscales y corrupción

PROCESO	TIPO DE RIESGO	RIESGO
Centralización de la información	Gestión	<p>R1. Posibilidad de afectación reputacional por el incumplimiento en la cobertura necesaria para generar el Estado de Situación Financiera y de Resultados Consolidados debido a limitaciones en el talento humano y en disponibilidad de recursos económicos, así como por cese de operaciones de la entidad sin información previa a la CGN.</p> <p>R2. Posibilidad de afectación reputacional por inexactitud en el reporte de la información para la generación de productos debido al desconocimiento del Régimen de Contabilidad Pública por parte de las entidades reportantes.</p>
	Corrupción	R3. Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio por omitir requerimientos formulados desde la CGN debido a intereses de la entidad contable pública y su reporte de la Información requerida por los analistas
Consolidación de la información	Gestión	R3. Posibilidad de afectaciones en la reputación por incumplimiento en la entrega de productos diferentes a los establecidos por ley debido a fallas en la planeación y/o falta de diligencia o destrezas del personal para la elaboración y revisión de documentos e informes y/o inconsistencias en la información reportada por las entidades y/o pérdida de la información elaborada por la CGN.
Gestión humana	Gestión	<p>R2. Posibilidad de afectación operacional por la ocurrencia de accidentes y/o enfermedades laborales debido a la falta de ejecución del SGSST</p> <p>R5. Posibilidad de afectación operacional por fuga de conocimiento de la entidad debido a falta de articulación del procedimiento de gestión del</p>

PROCESO	TIPO DE RIESGO	RIESGO
		conocimiento con otros procedimientos asociados a la desvinculación o movilidad administrativa
	Corrupción	R3. Posibilidad de incurrir en favorecimiento a un tercero, por medio de la selección o vinculación de personal a causa de un ajuste en los requisitos
Gestión Administrativa	Corrupción	R4. Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros, en los procesos contractuales por el direccionamiento en las condiciones del proceso, para favorecer a terceros, debido a intereses particulares o al uso indebido de la función pública o de la información.
Gestión de recursos financieros	Gestión	R1. Posibilidad de afectación operacional por expedición de documentos presupuestales con información errada debido a inexactitudes en la solicitud de documentos presupuestales (CDP Y RP)
	Corrupción	R3. Posibilidad de recibir o solicitar cualquier dádiva en la caja menor por desviación de los recursos asignados, debido a intereses particulares y presiones de terceros
Gestión TICS	Gestión	R1. Probabilidad de afectación operacional por la no ejecución del plan de adquisiciones del proceso debido a la falta de gestión a la solicitud presupuestal y que el personal del área carece de las competencias necesarias
	Corrupción	R2. Posibilidad de recibir o solicitar dádivas o beneficios a nombre propio o de terceros para favorecer intereses particulares por la utilización inapropiada de la información de la entidad debido a la no suscripción de los acuerdos de confidencialidad y de la aceptación formal de las políticas de seguridad, que controlen el acceso a la información conforme a las funciones y responsabilidades del personal R3. Posibilidad de incurrir en gastos de bienes y servicios tecnológicos que no se necesiten en la entidad para beneficio propio o de terceros por presiones indebidas o conflictos de interés debido a falta de ética

PROCESO	TIPO DE RIESGO	RIESGO
		por parte del servidor público o contratista responsable de gestionar el proceso de adquisición tecnológica
Gestión jurídica	Fiscales	R3. Posibilidad de efectos dañosos sobre recursos públicos por la caducidad de la acción de repetición debido a fallas en la gestión y trámite de los procesos judiciales.
Control y evaluación	Corrupción	R2. Posibilidad de recibir o solicitar dádiva o cualquier beneficio propio o de terceros en la elaboración de informes por omitir o adulterar información relevante frente a situaciones observadas en el desarrollo de las diferentes evaluaciones, auditorías y/o seguimientos establecidos en el Plan Anual de Auditorías y Seguimientos debido a la falta de ética profesional de los funcionarios y/o contratistas del GIT de Control Interno

Tabla 2. Muestra de riesgos de proyectos

PROYECTO	TIPO DE RIESGO	RIESGO
Mejoramiento del sistema contable público para atender los requerimientos de los usuarios estratégicos de la Contaduría General de la Nación Nacional	Proyectos	R4. Los documentos metodológicos no atienden específicamente las demandas de información R6. Dificultad en establecer los requerimientos de la interoperabilidad necesaria para los sistemas de información
Fortalecimiento de la regulación contable pública con los avances internacionales y el contexto del sector público Colombiano Nacional	Proyectos	R2. Omisión en la modificación de la regulación contable pública a partir del análisis de las modificaciones a los estándares internacionales de información financiera o a la regulación de carácter general que genera hechos económicos que requieren regularse contablemente
Fortalecimiento e Integración de los Sistemas	Proyectos	R1. Falta de cobertura de todos los temas y criterios normativos en la realización de

PROYECTO	TIPO DE RIESGO	RIESGO
de Gestión y Control de la CGN a través del Sistema Integrado de Gestión Institucional - SIGI Nacional		las evaluaciones periódicas realizadas al SIGI
Fortalecimiento de la plataforma tecnológica para la prestación de los servicios de la CGN Nacional	Proyectos	R3. Aumentos inesperados en la tasa representativa del mercado

Tabla 3. Muestra de riesgos de seguridad de la información

PROCESO	TIPO DE RIESGO	RIESGO
Centralización de la Información, Normalización y Culturización Contable, Consolidación de la Información, Gestión TICS	Seguridad de la Información	R1. Posibilidad de incumplimiento de las políticas de seguridad de la información por uso indebido de los derechos por parte de los usuarios a causa del desconocimiento de los procedimientos y Políticas de Seguridad de la Información y Seguridad Digital y su insuficiente apropiación
Centralización de la Información, Normalización y Culturización Contable, Consolidación de la Información, Gestión TICS	Seguridad de la Información	R2. Afectación del acceso a los sistemas y servicios de TI de la CGN por acciones indebidas de los funcionarios o contratistas con privilegios de acceso debido a la ausencia de implementación de procedimientos en la gestión de usuarios
Centralización de la Información, Normalización y Culturización Contable, Consolidación de la Información, Gestión TICS	Seguridad de la Información	R3. Perdida de confidencialidad, disponibilidad e integridad de la información de la CGN, por divulgación de procedimientos o información catalogada como reservada a los proveedores y/o contratistas, debido a la ausencia de requisitos de seguridad de la información en los contratos suscritos.
Gestión TICS	Seguridad de la Información	R4. Indisponibilidad de los servicios de TI causada por la interrupción en la operación de sus componentes, debido a la ausencia de pruebas, debilidades en la plataforma tecnológica o factores ambientales

PROCESO	TIPO DE RIESGO	RIESGO
Gestión TICS	Seguridad de la Información	R5. Perdida de confidencialidad, integridad y disponibilidad de los servicios de TI, por fuga o pérdida de información generada por código malicioso o accesos permitidos debido a la ausencia de políticas y controles restrictivos de descarga e instalación de software no autorizado.
Gestión TICS	Seguridad de la Información	R6. Afectación de la integridad y disponibilidad de la información y los servicios de TI, por el uso inadecuado de medios removibles y falta de control de acceso a sitios web debido a falta de restricciones en el control de dispositivos y de contenidos maliciosos