CONTADURÍA GENERAL DE LA NACIÓN
*Cuentas Claras, Estado Transparente*

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

## CUARTO TRIMESTRE DE 2025

## SEGUNDA LÍNEA DE DEFENSA
## GIT DE PLANEACIÓN
## GIT DE APOYO INFORMÁTICO

## Enero de 2026

Tabla de contenido

## 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 cuarto trimestre de 2025, realizado por la segunda línea de defensa.

El seguimiento y revisión de los riesgos 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. De igual manera, promover la cultura organizacional orientada al control y la prevención.

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

## 2. OBJETIVO

Presentar los resultados del monitoreo de riesgos de la CGN, con el fin de proporcionar una visión objetiva sobre la idoneidad de los controles asegurando la mitigación proactiva de amenazas, la protección del valor institucional y el cumplimiento de los objetivos estratégicos.

Este análisis se fundamenta en los lineamientos de la Política de Administración del Riesgo vigente, integrando la revisión de las matrices de riesgos (gestión, fiscales, corrupción y seguridad de la información) y validando la consistencia de los reportes generados por la primera línea de defensa.

A través de este ejercicio, la segunda línea de defensa identifica brechas, alerta sobre la posible materialización de eventos y formula conclusiones y recomendaciones orientadas al fortalecimiento del sistema de control interno y la mejora continua de la entidad.

## 3. ALCANCE

La revisión corresponde al periodo comprendido entre el 01 de octubre y el 31 de diciembre de 2025 y abarca todos los procesos de la entidad en las siguientes tipologías de riesgo:

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

## 4. METODOLOGÍA

El monitoreo de riesgos correspondiente al cuarto trimestre de 2025 se desarrolló mediante el análisis técnico de las matrices vigentes elaboradas a partir de la normatividad vigente (Guía DAFP V6 - administración del riesgo y diseño/evaluación de controles; Ley 87 de 1993 - evaluación y documentación del control y el MECI - monitoreo y actividades de control), contrastando el reporte de la primera línea de defensa frente a la aplicación de los controles. Para este ejercicio, la segunda línea de defensa tuvo en cuenta los siguientes componentes:

- Monitoreo de riesgos identificados: verificación de la vigencia y pertinencia de los riesgos frente al contexto institucional.
- Aplicación de controles: análisis de la ejecución real de las medidas de mitigación y su capacidad para reducir la probabilidad o el impacto.
- Cumplimiento de planes de acción: evaluación del cronograma y avance físico de las actividades orientadas a tratar riesgos que se encuentren clasificados en niveles de aceptación con la categoría "No aceptables".
- Materialización de riesgos: verificación de la ocurrencia de eventos de riesgo y la activación de los respectivos planes de contingencia.
- Gestión de novedades: reporte de cambios significativos en los procesos que afecten el perfil de riesgo institucional.

Dando cumplimiento al numeral 13 de la Política de Administración del Riesgo, el GIT de Planeación y el GIT de Apoyo Informático, en conjunto con el Oficial de Seguridad y Privacidad de la Información (OSPI), ejercieron su rol de supervisión mediante un muestreo representativo.

Para el cierre del cuarto trimestre de la vigencia 2025, se continuó con la técnica de muestreo acostumbrada, es decir, una muestra no probabilística de conveniencia, accidental o de oportunidad compuesta de la siguiente manera:

- 07 riesgos de gestión.
- 01 riesgo fiscal.
- 07 riesgos de corrupción (cobertura del 100% de la tipología).
- 05 riesgos de proyectos de inversión.
- 06 riesgos de seguridad de la información y seguridad digital.

(Para un análisis detallado de la muestra, remitirse al Anexo 1 del presente informe).

Este proceso de monitoreo fue realizado por la segunda línea de defensa y corresponde al cuarto trimestre de 2025 (cierre 31 de diciembre de 2025).

## 5. ACTUALIZACIÓN DE RIESGOS DE LA CGN

Durante la vigencia 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, a partir de la aplicación de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" – Versión 6 y lo establecido en la norma ISO/IEC 27001 junto con sus anexos, en la versión vigente.

Lo anterior dio como resultado un total de:

- 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.

- En el cuarto trimestre únicamente se actualizó el tercer control del riesgo número 3 del proceso misional Centralización de la Información.

- 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.

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

La revisión realizada por la segunda línea de defensa se estructuró en tres ejes de análisis: en primer lugar, los riesgos de gestión, fiscales y de corrupción; en segundo lugar, los componentes de seguridad de la información y seguridad digital; y finalmente, los riesgos asociados a los proyectos de inversión de la entidad.

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

Observaciones Generales:

- Oportunidad: se destaca que los procesos cumplieron con la entrega del monitoreo dentro de los plazos establecidos en el cronograma institucional.

- Gestión de evidencias: aunque se reportó el cumplimiento de las actividades de los planes de acción, se identificó, en algunos casos, una debilidad en el soporte documental, debido a la ausencia de evidencias cargadas en el repositorio definido.

- Materialización: durante el periodo analizado no se registraron eventos de materialización de riesgos en estas tipologías.

Observaciones Específicas:

- Riesgos de gestión: para la totalidad de riesgos analizados, se identificó la necesidad de fortalecer la triangulación entre el control, la ejecución y el soporte. De igual manera, las evidencias deben guardar una relación directa y unívoca con la descripción del control en la matriz. Por otro lado, para aquellos riesgos donde la evaluación del control se soporte en actas y/o ayudas de memoria, se recomienda precisar las fechas en las cuales se llevaron a cabo y adjuntarlas como documento soporte.

- Riesgos de corrupción: se observó un nivel de cumplimiento satisfactorio en cuanto a soportes y ejecución de planes de tratamiento. Se enfatiza que el control debe ser exhaustivo para todos los eventos definidos, limitando la aleatoriedad solo a los casos expresamente previstos en la metodología.

- Riesgos fiscales: a partir de la muestra definida, se analizó únicamente el riesgo fiscal denominado "Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública por el incumplimiento en la liquidación de sueldos y prestaciones sociales a causa de una falla humana en la aplicación del procedimiento" del proceso Gestión humana, el cual reportó la ejecución de los controles y la realización de las actividades del Plan de tratamiento del riesgo. No obstante, se recomienda adjuntar las evidencias que soporten las tareas descritas.

- Planes de acción para tratamiento de riesgos: para las actividades con cierre proyectado en 2026 (Proceso de Consolidación de la Información), se requiere un mayor nivel de detalle en el reporte de avance para garantizar una adecuada gestión y cumplimiento del plan propuesto.

### 6.2. Observaciones para riesgos de Seguridad de la información y Seguridad digital

Tras la validación efectuada en conjunto con el Oficial de Seguridad y el GIT de Apoyo Informático, se concluye:

- Cumplimiento normativo: los procesos ejecutaron las actividades de control conforme a los tiempos y aspectos técnicos de la política de seguridad.

- Gestión de continuidad: se advierte que, de los cuatro planes de acción

programados, se completaron tres. Queda como compromiso para el primer trimestre de 2026 la ejecución de las pruebas de restauración de cintas, elemento esencial para la resiliencia institucional ante desastres.

- Recomendación de segunda línea: se insta a los líderes de proceso a mantener una verificación rigurosa de los controles de acceso y cifrado, anticipándose a los criterios de validación de la segunda línea.

### 6.3. Observaciones para riesgos en proyectos de inversión

El análisis del comportamiento de los riesgos en la fase de operación 2025 arroja los siguientes resultados:

- Alineación estratégica: la ejecución de los controles de mitigación ha soportado adecuadamente el cumplimiento de las metas físicas y financieras de la vigencia.

- Cultura de monitoreo: se observa una disciplina adecuada en el reporte de tiempos y en la aplicación de medidas de mitigación.

- Sostenibilidad: se recomienda mantener el monitoreo permanente para prevenir contratiempos en la fase operativa de los proyectos, para asegurar que la gestión del riesgo actúe como un facilitador del gasto público eficiente.

## 7. CONCLUSIONES Y RECOMENDACIONES

1. Cumplimiento y reporte

- Conclusión: se destaca el compromiso de la primera línea de defensa, la cual realizó el reporte de monitoreo de riesgos de manera oportuna y dentro de los términos establecidos en el cronograma institucional.

- Recomendación: continuar con la cultura de reporte temprano para facilitar la consolidación de la información por parte de la segunda línea de defensa.

2. Fortalecimiento del control y evidencia

- Conclusión: en algunos de los riesgos analizados, el proceso de monitoreo requiere un mayor grado de trazabilidad, mediante la recolección de las evidencias y soportes que certifiquen tanto la vigencia de los controles como el progreso real de las acciones de mitigación.

- Recomendación: para todos los procesos analizados, se sugiere validar

que la información reportada trimestralmente coincida con las evidencias cargadas en el repositorio, asegurando así la integridad del sistema de control de riesgos, facilitando el análisis y construcción de los informes de seguimiento a los riesgos.

3. Materialización y comportamiento del riesgo

- Conclusión: no se reportó la materialización de riesgos durante este periodo. Sin embargo, es fundamental mantener la vigilancia activa ante posibles cambios en el entorno.

- Recomendación: monitorear permanentemente los factores de riesgo para ajustar o crear controles preventivos de manera anticipada, sin esperar a que el nivel de riesgo aumente.

4. Estado de los planes de acción de seguridad de la información y seguridad digital.

- Conclusión: el avance de los planes de acción es satisfactorio; de los cuatro proyectados, tres se han cumplido en su totalidad. Queda pendiente la ejecución de las pruebas de restauración de cintas, programadas para el primer trimestre de 2026.

- Recomendación: priorizar la ejecución de la actividad pendiente sobre cintas de respaldo para garantizar la integridad y disponibilidad de la información, conforme a la política de continuidad del negocio.

5. Aspectos a destacar frente al informe del tercer trimestre de 2025.

- Soportes del monitoreo: se fortaleció la presentación de evidencias que respaldan la aplicación de los controles a los riesgos de las diferentes tipologías.

- Evidencias periodo evaluado: se identificó que la primera línea de defensa acogió la recomendación planteada en el anterior informe, de incluir la evidencia únicamente al periodo analizado.

- Seguimiento planes de acción para el tratamiento de riesgos: se implementó la recomendación de efectuar un seguimiento a las acciones incluidas en los planes para un adecuado tratamiento de los riesgos.

# ANEXO 1

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

| PROCESO | TIPO DE RIESGO | RIESGO |
|---|---|---|
| Normalización y culturización contable | Gestión | R1. Posibilidad de afectación reputacional por inoportunidad en la emisión de conceptos y solución de consultas debido a la falta de seguimiento a la oportunidad en la emisión de conceptos y solución de consultas; a la falta de competencia del recurso humano para la gestión del proceso; o a la necesidad de profundización en el estudio, dada la complejidad del concepto a emitir. |
| Centralización de la información | Gestión | 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. |
| | 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 | R2. Posibilidad de afectación reputacional por inoportunidad en la entrega de los informes establecidos por ley (Balance General de la Nación y de la Hacienda pública, CLC, BDME, ECIC, Certificado de Excedentes financieros, Inventario de entidades) 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 | R1. Posibilidad de afectación reputacional por el incumplimiento en las actividades del plan estratégico de talento humano debido a fallas en la ejecución del plan<br><br>R5. Posibilidad de afectación operacional por fuga de conocimiento de la entidad debido a falta de articulación del procedimiento de gestión del |

| 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 humana | Fiscales | R4. Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública por el incumplimiento en la liquidación de sueldos y prestaciones sociales a causa de una falla humana en la aplicación del procedimiento |
| 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 | R2. Posibilidad de afectación reputacional por registro incorrecto de los hechos económicos en el sistema financiero debido al reconocimiento contable inadecuado o duplicado. |
| | 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 dadivas 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<br><br>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 |
| 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 |
|---|---|---|
| Capacitación, Divulgación y Asistencia Técnica en el Modelo Colombiano de Regulación Contable Pública Nacional | Proyectos | R3. Actualización de la regulación contable pública por cambios en el entorno jurídico, económico y social del sector público colombiano, y por los cambios en las tendencias de la regulación contable a nivel internacional |
| Mejoramiento del sistema contable público para atender los requerimientos de los usuarios estratégicos de la Contaduría General de la Nación Nacional | Proyectos | R1. Dificultad en la viabilización del Proyecto de Inversión<br><br>R4. Los documentos metodológicos no atienden específicamente las demandas de información |
| Fortalecimiento de la regulación contable pública con los avances internacionales y el contexto del sector público Colombiano Nacional | Proyectos | R3. Documentos metodológicos que no interpreten adecuadamente la aplicación de regulación contable pública expedida a los casos específicos de las entidades reguladas |
| Fortalecimiento e Integración de los Sistemas de Gestión y Control de la CGN a través del Sistema Integrado de Gestión Institucional - SIGI Nacional | 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 |
|---|---|---|
| Oficial de seguridad y privacidad de la información, Coordinador(a) GIT de Apoyo Informático | Seguridad de la Información | R7. Perdida de confidencialidad, integridad y disponibilidad de la información, por sustracción de información o ciberataques debido a la inadecuada manipulación de los medios o falta de integridad por parte de funcionarios, contratistas o terceros |
| Oficial de seguridad y privacidad de la información, Coordinador(a) GIT de Apoyo Informático | Seguridad de la Información | R8. Perdida de disponibilidad de los servicios de TI por ataques informáticos internos o externos a la infraestructura tecnológica debido al acceso no autorizado |
| Oficial de seguridad y privacidad de la información, Coordinador(a) GIT de Apoyo Informático | Seguridad de la Información | R9. Afectación a la disponibilidad de los servicios de red y/o comunicaciones en la CGN, por fallas de los servicios ofrecidos por el proveedor debido a falta de respaldo de los servicios de red o comunicaciones o por incumplimiento de los acuerdos de nivel de servicio pactados con el proveedor. |
| Oficial de seguridad y privacidad de la información, Coordinador(a) GIT de Apoyo Informático | Seguridad de la Información | R10. Indisponibilidad de los servicios de red por ataques de denegación de servicios (DoS) o fallas en los equipos, debido a la inadecuada gestión o monitoreo |
| Subcontador(a) de Centralización de la Información, Subcontador(a) General y de Investigación, Subcontador(a) de Consolidación de la Información, Coordinador(a) GIT de Apoyo Informático | Seguridad de la Información | R11. Posibilidad de acceso no autorizado, por inadecuada gestión de contraseñas en las diferentes plataformas, debido a falta de notificación de novedades y apropiación de los usuarios |

| PROCESO | TIPO DE RIESGO | RIESGO |
|---|---|---|
| Oficial de seguridad y privacidad de la información, Coordinador(a) GIT de Apoyo Informático | Seguridad de la Información | R 12. Pérdida de confidencialidad, integridad y disponibilidad de los datos por interceptación, modificación o divulgación durante el proceso de transferencia debido a la falta de mecanismos de autenticación, cifrado o canales seguros |