CONTADURÍA GENERAL DE LA NACIÓN
Cuentas Claras, Estado Transparente

**UNIDAD ADMINISTRATIVA ESPECIAL**
**CONTADURÍA GENERAL DE LA NACIÓN - CGN**

**GRUPO INTERNO DE TRABAJO DE APOYO INFORMÁTICO**

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2026

**DICIEMBRE DE 2025**

Dirección: Calle 26 # 69 - 76 | Edificio Elemento
Torre 1 (Aire) - Piso 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

## CONTROL DE CAMBIOS

| VERSIÓN | SECCIÓN | TIPO | FECHA (DD/MM /AAAA) | AUTOR | OBSERVACIONES |
|---|---|---|---|---|---|
| 1.0 | Todas | Creación | 29-12-2023 | Git de Apoyo Informático | Elaboración del plan |
| 2.0 | Todas | Actualización | 15-11-2024 | GIT de Apoyo Informático | Actualización del plan |
| 3.0 | Todas | Actualización | 9-12-2025 | GIT de Apoyo Informático | Actualización del plan |

# Contenido

## 1. Introducción

La Contaduría General de la Nación, en adelante CGN, al igual que la mayoría de las entidades públicas en Colombia mueve gran parte de su operación misional en un entorno cada vez más digital y amenazante. Los riesgos asociados con violaciones de seguridad, pérdida de datos o interrupciones en los servicios pueden tener un impacto directo en su capacidad de operar de manera eficiente y cumplir con sus metas estratégicas.

La pérdida de la confianza de los grupos de valor debido a brechas de seguridad puede resultar en una disminución significativa de las oportunidades institucionales, por lo tanto, puede afectar negativamente los objetivos estratégicos relacionados con el fortalecimiento, crecimiento y expansión.

La gestión proactiva de riesgos de seguridad y privacidad de la información no solo ayuda a cumplir con las regulaciones vigentes, sino que también demuestra un compromiso serio con la responsabilidad institucional y la protección de los intereses de todas las partes involucradas, lo que se alinea directamente con los objetivos estratégicos centrados en la integridad y la excelencia operativa.

En cumplimiento del Decreto 1008 de 2018 para el desarrollo del habilitador transversal "Seguridad de la Información" de la Política de Gobierno Digital, así como para dar cumplimiento a la Resolución 500 de 2021 que da lineamientos para el desarrollo de la estrategia de seguridad digital y conforme al Decreto 767 de 2022, expedidos por Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que desarrolla el habilitador de Seguridad y Privacidad de la Información y se estructura este documento en el contexto de la CGN. De igual manera, el presente documento se alinea con las disposiciones prescritas en los siguientes documentos: CONPES 3701 de 2011, Lineamiento de Políticas de Ciberseguridad y Ciberdefensa; CONPES 3854 de 2016, Política Nacional de SeguridadDigital; CONPES 3975 de 2019, Política Nacional para la Transformación Digital e Inteligencia Digital; y CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad Digital; con lo cual se define de manera integral en el presente documentoel Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para la vigencia 2026.

## 2. Objetivo

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece los lineamientos metodológicos para la administración de los riesgos de seguridad de la información que permitan fortalecer el enfoque preventivo para mitigar los riesgos de Seguridad Digital que superan el nivel de riesgo aceptable para la Entidad, y que su materialización pueda impactar el logro de los objetivos estratégicos de la CGN.

## 3. Alcance

La gestión de riesgos de seguridad de la información aplica a todos los activos de información que forman parte de los procesos institucionales de la CGN y demás partes interesadas que comparten, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de activo de información, identificados en el Sistema de Gestión de la Seguridad de la Información, en adelante SGSI, de la entidad.

Inicia con la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, continua con la ejecución del Plan y finaliza con el seguimiento y evaluación de la gestión realizada.

Aplica a todos los activos de información creados, procesados o utilizados sin importar el medio, formato o presentación y lugar en el cual se encuentre.

## 4. Definiciones

**Activos de información:** se refiere a cualquier dato o recurso vinculado al procesamiento de la información (como sistemas, dispositivos de almacenamiento, infraestructura física locativa y de TI o recursos humanos) que posea un valor significativo para la organización.

**Amenaza:** una amenaza informática es toda circunstancia, evento o acción que tiene el potencial de causar daño, degradar la seguridad o comprometer activos de la entidad. Estas amenazas pueden surgir tanto de fuentes internas como externas y pueden ser intencionadas o accidentales.

**CIGD:** sigla de Comité Institucional de Gestión y Desempeño

**Confidencialidad:** es un principio de seguridad de la información que garantiza que los datos sensibles o privados se mantengan protegidos y solo estén disponibles para aquellos usuarios autorizados que tienen permiso explícito para acceder a ellos.

**Control:** es una medida o procedimiento implementado para proteger los activos, minimizar riesgos y asegurar el cumplimiento de políticas de seguridad. Estos controles pueden ser tecnológicos, físicos o de procedimiento, diseñados para mitigar amenazas y garantizar la confidencialidad, integridad y disponibilidad de la información.

**Disponibilidad:** es un principio de seguridad de la información que se refiere a la garantía de que los datos estén accesibles y disponibles para aquellos que tienen autorización para utilizarlos, en el momento en que se necesitan. Esto implica asegurar que los sistemas y recursos estén operativos y funcionando correctamente para permitir el acceso a la información cuando sea requerida.

**GIT:** sigla de Grupo Interno de Trabajo.

**Incidente de seguridad de la información:** es un evento que compromete la confidencialidad, integridad o disponibilidad de los datos o sistemas de una organización. Estos incidentes pueden ser intencionados o accidentales e incluyen acciones no autorizadas, fallos en la seguridad, intrusiones o pérdidas de datos que representan una amenaza para la seguridad de la información.

**Integridad:** es un principio de seguridad de la información que se refiere a la calidad de los datos que se encuentran completos, precisos y no han sido modificados de manera no autorizada. 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.

**MINTIC:** sigla del Ministerio de Tecnologías de la Información y las Comunicaciones.

**MSPI:** sigla del Modelo de Seguridad y Privacidad de la Información.

**PTRSPI:** sigla del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

**Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales (tomado de PLAN DE TRATAMIETO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MinTIC)

**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. (ISO/IEC 27000).

**Seguridad de la información:** preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

**SGD:** sigla de Sistema de Gestión y Desempeño

**SGSI**: sigla de Sistema de Gestión de la Seguridad de la Información.

**TI: Sigla Tecnologías de la información**

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

## 5. Condiciones generales

La Alta Dirección respalda activamente la gestión de riesgos de seguridad y privacidad de la información mediante el cumplimiento de la Política de Privacidad Y Protección de Datos, la Estrategia de Seguridad Digital, la implementación del SGSI y la adopción del marco regulatorio correspondiente.

En la preparación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en adelante PTRSPI, de la CGN, además, seda enfoque en la alineación de los procesos y la evaluación interna a través del instrumento de autodiagnóstico del MSPI del MINTIC, con el fin de identificar y aplicarlas actualizaciones pertinentes en este documento.

## 6. Estrategias de cumplimiento

La CGN, mediante la adopción e implementación del MSPI enmarcado en el SGSI, protege, preserva y gestiona la confidencialidad, integridad y disponibilidad de la información, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales reduciendo la probabilidad de ocurrencia de incidentes y/o las consecuencias de su materialización.

Para lograr el cumplimiento del PTRSPI se definen las siguientes estrategias enmarcadas en el ciclo de mejora continua PHVA:

1. Definir las actividades del *planear* de tratamiento de riesgos.
2. Definir las actividades del *hacer* de tratamiento de riesgos.
3. Definir las actividades del *verificar* de tratamiento de riesgos.

4. Definir las actividades del *actuar* de tratamiento de riesgos.

## 7. Roles y responsabilidades

| Rol | | Responsabilidad |
|---|---|---|
| Rol Estratégico | Comité Institucional de Gestión y Desempeño | - Aprobar el PTRSPI.<br>- Aprobar la Matriz de Tratamiento de Riesgos de Seguridad<br>- Tomar decisiones sobre los asuntos de la gestión de riesgos de seguridad. |
| Rol Táctico | Oficial de Seguridad de la Información o quien haga sus veces.<br><br>Equipo Seguridad de la Información del GIT de Apoyo Informático | - Preparar, presentar y hacer seguimiento a la Matriz de Tratamiento de Riesgos de Seguridad.<br>- Gestionar los activos de información<br>- Apoyar a los responsables de los activos de información en la identificación de los riesgos asociados.<br>- Realizar seguimiento al cumplimiento del PTRSPI por parte de los responsables. |
| Rol Funcional y operativo | Equipo operativo de apoyo para el Oficial de Seguridad y Privacidad de la Información<br><br>Equipo Seguridad de a Información del GIT de Apoyo Informático | - Informar sobre la gestión del plan de seguridad y privacidad de la información del proceso.<br>- Implementar controles que ayuden a mitigar los riesgos de seguridad de la información y seguridad digital.<br>- Velar por la protección de los activos de información del proceso<br>- Realizar revisiones periódicas al Modelo de Seguridad y Privacidad de la Información (MSPI) |
| | Funcionarios y colaboradores de la CGN | - Cumplir con las disposiciones establecidas en las políticas de seguridad de la información y seguridad digital.<br>- Velar por la protección de los activos de información del proceso<br>- Apoyar el mantenimiento y mejora continua del Sistema Integrado de Gestión Institucional (SGSI) en el área |

## 8. Desarrollo del Plan de Tratamiento de Riesgos

El PTRSPI de la CGN tiene como propósito definir las actividades para la identificación, evaluación, tratamiento y aceptación de los riesgos de seguridad y privacidad de la información asociados a los activos de información críticos de la entidad, para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados.

Para su desarrollo se toma como base el documento Política de administración de riesgos de la CGN, basado en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública.

De igual manera la CGN establece una revisión anual de los riesgos con el propósito de identificar nuevos potenciales riesgos o eliminar riesgos cuyo potencial de materialización sea mínimo o se puedan asumir.

**Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información:**

La CGN define las actividades de actualización para el año 2026, basada en el análisis de la identificación, de las causas y de las acciones para mitigar la causa raíz, así como en monitoreo y la revisión periódica de la aplicación de los controles establecidos para la gestión de los riesgos de seguridad de la información y seguridad digital. Dichas actividades de actualización se definen a continuación:

| No. | Actividad | Actividades Por Ejecutar | Tema | Producto | Responsable | Tiempo estimado |
|---|---|---|---|---|---|---|
| 1 | Actualización de lineamientos de riesgos | Apoyar en procesos de actualización metodológica para la gestión de riesgos | lineamientos de riesgos | recomendaciones | Equipo Seguridad de la Información del GIT de Apoyo Informático<br><br>Oficial de seguridad Gestión TICs | 1er Semestre |
| 2 | Identificación de riesgos de Seguridad de la Información, digital y continuidad | Contexto, identificación, análisis y evaluación de riesgos | Identificación y evaluación de riesgos | Matriz de riesgos de seguridad de la información y seguridad digital actualizada con controles (Incluir las evidencias) | | 1er Semestre |
| 3 | Revisión y actualización de riesgos de Seguridad de la Información y su tratamiento | Seguimiento Implementación de controles y planes de tratamiento | Controles y tratamiento de riesgos | | | 1er y 2do Semestre |
| 4 | Valoración de riesgos y acciones de SI | Valoración de riesgo | Valoración de riesgo | | | 1er Semestre |
| 5 | Aceptación de riesgos identificados por CIGD | Aceptación y aprobación de riesgos identificados y planes de tratamiento | aceptación y aprobación de riesgos | | | 1er Semestre |

| No. | Actividad | Actividades Por Ejecutar | Tema | Producto | Responsable | Tiempo estimado |
|---|---|---|---|---|---|---|
| 6 | Publicación | Publicación mapa de riesgos | Publicación de última versión | | | 1er Semestre |
| 7 | Sensibilización | Socialización de lineamientos y manejo de matriz de riesgos de Seguridad | Socialización | Evidencia de sensibilización | | 1er y 2do Semestre |
| 8 | Seguimiento y monitoreo del tratamiento | Seguimiento implementación de controles y planes de tratamiento (verificación evidencia) | Seguimiento | Evidencia del seguimiento del tratamiento | | Trimestral |
| 9 | Mejoramiento | Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de controles y planes de mejoramiento | Mejora | Evidencia del mejoramiento | | 2do Semestre |
| 10 | Monitoreo y revisión | Medición, presentación y reporte de indicadores | Monitoreo | Entregable y Evidencia | | Trimestral |

Fuente: propia

## 9. Seguimiento al plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia anterior

El seguimiento del plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 se presenta a continuación:

| No. | Actividad | Actividades Por Ejecutar | Tema | Producto | Responsable | Tiempo estimado | Descripción Avance |
|---|---|---|---|---|---|---|---|
| 1 | Actualización de lineamientos de riesgos | Apoyar en procesos de actualización metodológica para la gestión de riesgos | lineamientos de riesgos | Recomendaciones | Oficial de seguridad Gestión TICs | 1er Semestre | Matriz de riesgos de seguridad de la información y seguridad digital actualizada a versión 6 de la Guía del DAFP y alineada a los controles de la norma ISO/IEC 27001:2022 aprobación comité CICII 21 de agosto y publicada |
| 2 | Identificación de riesgos de Seguridad de la Información, digital y continuidad | Contexto, identificación, análisis y evaluación de riesgos | Identificación y evaluación de riesgos | Matriz de riesgos de seguridad de la información y seguridad digital actualizada | | 1er Semestre | realizado |

| No. | Actividad | Actividades Por Ejecutar | Tema | Producto | Responsable | Tiempo estimado | Descripción Avance |
|---|---|---|---|---|---|---|---|
| 3 | Revisión y actualización de riesgos de Seguridad de la Información y su tratamiento | Seguimiento Implementación de controles y planes de tratamiento | Controles y tratamiento de riesgos | con controles (Incluir las evidencias) | | 1er y 2do Semestre | realizado |
| 4 | Valoración de riesgos y acciones de SI | Valoración de riesgo | Valoración de riesgo | | | 1er Semestre | realizado |
| 5 | Aceptación de riesgos identificados por CIGD | Aceptación y aprobación de riesgos identificados y planes de tratamiento | aceptación y aprobación de riesgos | | | 1er Semestre | aprobada 21 de agosto 2025 |
| 6 | Publicación | Publicación mapa de riesgos | Publicación de última versión | | | 1er Semestre | publicada en página web e intranet |
| 7 | Sensibilización | Socialización de lineamientos y manejo de matriz de riesgos de Seguridad | Socialización | Evidencia de sensibilización | | 1er y 2do Semestre | Socialización matriz definitiva |
| 8 | Seguimiento y monitoreo del tratamiento | Seguimiento implementación de controles y planes de tratamiento (verificación evidencia) | Seguimiento | Evidencia del seguimiento del tratamiento | | Trimestral | seguimiento con corte a 30 de septiembre |
| 9 | Mejoramiento | Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de controles y planes de mejoramiento | Mejora | Evidencia del mejoramiento | | 2do Semestre | Controles aplicados de la versión 27001:2022 |
| 10 | Monitoreo y revisión | Medición, presentación y reporte de indicadores | Monitoreo | Entregable y Evidencia | | Trimestral | Medición asociada a Gestión de incidentes de seguridad de la información - Indicador (Número de eventos o incidentes cerrados / Número de eventos o incidentes reportados) *100 |

Fuente: Propia

## 10. Anexos

Archivo Excel Matriz de Riesgos de Seguridad de la Información – Seguridad Digital publicado en el siguiente enlace:

https://www.contaduria.gov.co/documents/d/guest/matriz-de-riesgos-sisd-21082025

## 11. Bibliografía

MINTIC, (2024). Política de gobierno digital. Recuperado el 22 de octubre de 2024 de https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

DAFP, (2022). Guía para la administración de riesgos. Recuperado el 4 de diciembre de 2024

https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

Elaboró: Martha Patricia Zornosa G.
Revisó: Jamir Mosquera R./Martha Patricia Zornosa G.
Aprobó: Freddy Armando Castaño Pineda