

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

**GRUPO INTERNO DE TRABAJO DE APOYO INFORMÁTICO**

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**DICIEMBRE DE 2023**

## **CONTROL DE CAMBIOS**

<b>VERSIÓN</b>	<b>SECCIÓN</b>	<b>TIPO</b>	<b>FECHA (DD/M M/AAA A)</b>	<b>AUTOR</b>	<b>OBSERVACIONES</b>
1.0	Todas	Creación	06-12-2018	Git de Apoyo Informático	Elaboración del plan
2.0	Todas	Actualización	27-12-2019	Git de Apoyo Informático	Actualización del plan vigencia 2020
3.0	Todas	Actualización	03-12-2020	Git de Apoyo Informático	Actualización del plan vigencia 2021
4.0	Todas	Actualización	12-11-2021	Git de Apoyo Informático	Actualización del plan vigencia 2022
5.0	6,9	Actualización	13-10-2022	Git de Apoyo Informático	Actualización del plan vigencia 2023
6.0	7,8,9	Actualización	30/11/2023	Git de Apoyo Informático	Actualización de roles, funciones y plan vigencia 2024

## Contenido

1.	Introducción .....	4
2.	Objetivo .....	5
3.	Alcance .....	5
4.	Definiciones .....	5
5.	Condiciones generales .....	7
6.	Estrategias de cumplimiento .....	7
7.	Roles y responsabilidades .....	8
8.	Funciones .....	8
9.	Plan de Seguridad y Privacidad de la Información .....	10
10.	Bibliografía: .....	13

## 1. Introducción

La Contaduría General de la Nación 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 MinTIC que desarrolla el habilitador de Seguridad y Privacidad de la Información en concordancia con los lineamientos de los documentos CONPES 3701 de 2011 Lineamiento de Políticas de Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad Digital, CONPES 3975 de 2019 Política Nacional para la Transformación Digital e Inteligencia Digital, CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital.

Dando cumplimiento a lo anterior define el Plan de Seguridad y Privacidad de la Información – Plan PSI en el marco del Decreto 612 de 2018 – Plan de Acción y Planes Institucionales, para la vigencia 2024.

## 2. Objetivo

Establecer las medidas, actividades y controles necesarios para adelantar la gestión de la seguridad y privacidad de la información (SPI) de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información, la norma ISO NTC/IEC ISO 27001:2013, la estrategia de Seguridad Digital y Continuidad de la operación de la U.A.E Contaduría General de la Nación – CGN para asegurar la confidencialidad, integridad y disponibilidad de la información para mitigar riesgos de seguridad y cumplir con regulaciones relacionadas.

## 3. Alcance

La gestión de la seguridad y privacidad de la información aplica a todos los procesos institucionales de la U.A.E Contaduría General de la Nación y demás partes interesadas que comparten, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de información, ya sea interna o externa, así como las actividades pertinentes que se consideren fundamentales para determinar la estrategia de implementación de los controles de seguridad requeridos para el adecuado funcionamiento del SGSI en la entidad.

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

Aplica a toda información creada, procesada o utilizada sin importar el medio, formato o presentación y lugar en el cual se encuentre.

## 4. Definiciones

**Activos de información:** activo de información es 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 la misma.

**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 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 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.

**Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales (tomado de PLAN DE TRATAMIENTO 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.

**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 seguridad y privacidad de la información (SPI) mediante el cumplimiento de la política de privacidad y protección de datos, la Estrategia de Seguridad Digital, la gestión de riesgos, la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y la adopción del marco regulatorio correspondiente. Además, se enfoca en la alineación de los procesos y la evaluación interna a través del instrumento de autodiagnóstico del MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones, con el fin de identificar y aplicar las actualizaciones pertinentes en este documento.

En la preparación del plan de seguridad y privacidad de la información de la Contaduría General de la Nación, se siguieron los lineamientos establecidos en el Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en Entidades Públicas (Anexo Técnico No. 4 - DAFP), expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones. Además, se consideró la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la Información, así como el Diseño de Controles en Entidades Públicas, emitidos por el Departamento Administrativo de la Función Pública (DAFP).

## 6. Estrategias de cumplimiento

La Contaduría General de la Nación, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información - SGSI, protege, preserva y gestiona la confidencialidad, integridad, 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 dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua.

Para lograr el cumplimiento del Plan se definen las siguientes estrategias:

1. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en los lineamientos de la Seguridad y Privacidad de la Información.
2. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad de la información de la CGN.
3. Gestionar los riesgos de SPI y Seguridad Digital de manera integral.
4. Mitigar los incidentes de Seguridad de la Información y Seguridad Digital de forma efectiva, eficaz y eficiente.
5. Fomentar la concienciación sobre el uso y la importancia de la Seguridad y Privacidad de la Información como un elemento transversal en la CGN.
6. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

## 7. Roles y responsabilidades

Rol		Responsabilidad
Rol Estratégico	Comité Institucional de Gestión y Desempeño	<ul style="list-style-type: none"> <li>- Aprobar el Plan Seguridad y privacidad de la información.</li> <li>- Tomar decisiones sobre los asuntos de la seguridad de la información y seguridad digital</li> </ul>
Rol Táctico	Oficial de Seguridad o quien haga sus veces.	<ul style="list-style-type: none"> <li>- Preparar, presentar y hacer seguimiento al Plan Seguridad y privacidad de la información.</li> <li>- Velar por la efectividad de las políticas de seguridad de la información y seguridad digital.</li> <li>- Gestionar los activos de información</li> </ul>
Rol Funcional y operativo	GIT Apoyo Informático	<ul style="list-style-type: none"> <li>- Informar sobre la gestión del Plan de Seguridad y privacidad de la información del proceso.</li> <li>- Implementar controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.</li> <li>- Velar por la protección de los activos de información del proceso</li> </ul>
	Líderes de Procesos	<ul style="list-style-type: none"> <li>- Participar y apoyar la gestión del Plan de Seguridad y privacidad de la información.</li> <li>- Velar por la protección de los activos de información del proceso</li> <li>- Aplicar y promover los controles y buenas prácticas de seguridad de la información y seguridad digital.</li> </ul>

## 8. Funciones

### Comité Institucional de Gestión y Desempeño

Las funciones y responsabilidades en los temas de Seguridad de la Información y seguridad digital son desarrolladas por el Comité Institucional de Gestión y Desempeño mediante Resolución número 193 del 19 de junio 2019.

## Alta Dirección

- Aprobar anualmente o cuando se requiera la Política de Seguridad de la Información de la CGN
- Aprobar los objetivos de seguridad de la información, los cuales estarán alineados con los objetivos estratégicos de la entidad.
- Asignar y aprobar el presupuesto necesario para el normal funcionamiento del SGSI.
- Proporcionar los recursos necesarios para la ejecución y desarrollo de las actividades del SGSI.
- Promover activamente una cultura de seguridad y privacidad de la información basada en la mitigación de los riesgos para la entidad.

## Oficial de Seguridad o quien haga sus veces:

Tiene el rol del administrador del SGSI y es el responsable de:

- Realizar seguimiento al cumplimiento de los lineamientos y políticas del SGSI.
- Revisar y proponer las políticas, planes, programas, procedimientos en materia de seguridad de la información y digital para la aplicación de controles en el sistema.
- Realizar revisiones periódicas al SGSI y definir acciones para la mejora continua.
- Asegurar el cumplimiento de las políticas, normas, procedimientos, y demás lineamientos en materia de seguridad de la información y digital.
- Atender los eventos e incidentes de seguridad de la información y digital
- Recomendar y aplicar acciones de mejora al SGSI.
- Gestionar el tratamiento de riesgos y controlar las acciones de seguridad de la información y digital
- Definición de indicadores y su seguimiento.
- Gestionar los activos de información.

## Líderes de procesos:

El papel de los líderes de procesos en la ejecución del plan de revisión y seguimiento del Sistema de Gestión de Seguridad de la Información (SGSI) es fundamental, ya que son responsables de:

- Seguimiento a la ejecución de los planes de tratamiento de riesgos en seguridad de la información.
- Actualización de activos de información.
- Revisión y cumplimiento de los procedimientos, controles y políticas del SGSI.

### **Coordinador de GIT de Apoyo Informático:**

El GIT de apoyo informático y su equipo de trabajo serán los responsables de los controles técnicos de seguridad de la información:

- Cierre de vulnerabilidades técnicas y su seguimiento.
- Proporcionar la información de indicadores de seguridad de la información.
- Apoyar la atención y gestión de los eventos e incidentes de seguridad de la información y digital
- Gestionar los riesgos de seguridad de la información del proceso Gestión Tics.
- Establecer controles de seguridad de la información y digital en los servicios que presta el GIT de apoyo informático para asegurar la confidencialidad, disponibilidad e integridad de la información.
- Velar por la protección de los activos de información del GIT.

### **Funcionarios y Contratistas**

- Adoptar las políticas y procedimientos definidos para el sostenimiento del SGSI.
- Mantener la confidencialidad e integridad de la información que reciben, generan y procesan en la CGN.
- Hacer buen uso de los activos de información de la entidad.
- Respetar la legislación y regulación vigente.
- Notificar a la cuenta de correo electrónico [seguridadinformatica@contaduria.gov.co](mailto:seguridadinformatica@contaduria.gov.co) los eventos o incidentes de seguridad de información, así como cualquier eventualidad sospechosa que pueda poner en riesgo la continuidad de las operaciones de la CGN.

## **9. Plan de Seguridad y Privacidad de la Información**

El Plan de Seguridad y Privacidad de la Información de la CGN tiene como propósito definir las actividades para la operación, evaluación y mejora de la Seguridad y

Privacidad de la Información con énfasis en la gestión de activos de información, riesgos, toma de conciencia, protección de datos y seguridad digital institucional.

El seguimiento de la gestión del Plan de Seguridad de la Información 2024 se presenta al Comité Institucional de Gestión y Desempeño – CIGD, y define las acciones a seguir para su cumplimiento.

El Plan de Seguridad y privacidad de la información, comprende las siguientes actividades:

No.	Estrategia	Tema	Actividades Por Ejecutar	Producto	Tiempo estimado	Responsable		
1	Liderazgo de Seguridad de la Información	Diagnóstico o MSPI	Realizar actualización de Matriz del MSPI	Matriz de diagnóstico actualizada.	2do Semestre	Proceso Gestión TICs		
2		Declaración de Aplicabilidad	Revisión y actualización si es necesario de la declaración de aplicabilidad	Declaración de aplicabilidad actualizada		Proceso Gestión TICs		
3		Manual de políticas de seguridad de la información	Realizar la revisión y actualización del documento Manual de Políticas de Seguridad de la Información	Manual de políticas actualizado.		Alta Dirección Proceso Gestión TICs Planeación Integral		
4		Gestión de activos	Activos de información	Revisar, identificar, actualizar y aprobar inventario de Activos de Información de la CGN.		Matriz de activos de seguridad de la información y seguridad digital actualizada y aprobada	1er Semestre	Gestión Tics Planeación Integral Todos los procesos del alcance del SGSI
5		Gestión de riesgos	Riesgos de Seguridad de Información y	Revisar, valorar y clasificar los riesgos asociados a los activos de información		Matriz de riesgos de seguridad de la información y seguridad	1er Semestre	

No.	Estrategia	Tema	Actividades Por Ejecutar	Producto	Tiempo estimado	Responsable
6		Seguridad digital	Revisar y actualizar el tratamiento de riesgos de seguridad de la información y seguridad digital	digital actualizada		
7			Realizar seguimiento al tratamiento y control de acciones de los riesgos de seguridad de la información y seguridad digital			
8	Gestión de controles	Documentos del SGSI	Revisar, actualizar y gestionar los documentos del SGSI	Documentos del SGSI actualizados	2do Semestre	Gestión Tics Planeación Integral Todos los procesos del alcance del SGSI Secretaría General
9	Gestión de vulnerabilidades	Vulnerabilidades	Ejecución de pruebas de seguridad (análisis de vulnerabilidades) al menos una vez al año.	Informe de resultados de los test y retest de vulnerabilidad	1er y 2do Semestre	Gestión TICs Secretaría General
10			Realizar seguimiento, cierre y retest de las vulnerabilidades.			

No.	Estrategia	Tema	Actividades Por Ejecutar	Producto	Tiempo estimado	Responsable
11	Gestión de incidentes	Eventos e incidentes de Seguridad de la Información y Seguridad Digital	Revisar y actualizar el procedimiento de Gestión de Incidentes de seguridad de la información.	Procedimiento de gestión de incidentes actualizado	1er Semestre	Proceso Gestión TICs
12		Concientización de Seguridad de la Información y Seguridad Digital	Sensibilizar a los servidores y colaboradores de la CGN en el reporte y manejo de eventos de incidentes de Seguridad de la Información.	Sensibilización en temas de eventos e incidentes de seguridad de la información.		Planeación Integral Secretaría General
13	Plan de concientización, socialización y sensibilización	Concientización de Seguridad de la Información y Seguridad Digital	Realizar jornadas de sensibilización al personal de la CGN	Evidencias de las actividades desarrolladas	2do Semestre	Proceso Gestión TICs

## 10. Bibliografía:

MINTIC, (2021). Plan Estratégico de Seguridad de la Información (PESI). Recuperado el 15 de marzo de 2022 de [https://gobiernodigital.mintic.gov.co/692/articles-272948\\_recurso\\_1.zip](https://gobiernodigital.mintic.gov.co/692/articles-272948_recurso_1.zip)

MINTIC, (2021). Política de gobierno digital. Recuperado el 10 de junio de 2022 de <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/>

Función Pública, (2018). Decreto 612 de 2018, Plan de Seguridad y Privacidad de la Información, Recuperado el 10 de abril de 2020 de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85742>

Elaboró: Oralía Franco Goez / César Meza Gonzáles  
Revisó: Martha Patricia Zornosa G.  
Aprobó: Jamir Mosquera Rubio