UNIDAD ADMINISTRATIVA
ESPECIAL CONTADURIA
GENERAL DE LA NACIÓN

GRUPO INTERNO DE
TRABAJO DE APOYO
INFORMÁTICO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2023

BOGOTA, NOVIEMBRE DE 2022

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La Contaduría General de la Nación dando alcance al cumplimiento del Decreto 1008 de 2018 para el desarrollo del habilitador transversal "Seguridad de la Información" de la Política de Gobierno Digital; así mismo el Decreto 1499 de 2017 determina el cumplimiento institucional de las Políticas de Gobierno y Seguridad Digital en relación con el habilitador "Seguridad de la Información" conforme a la Resolución 500 de 2021 (MinTIC) y la Política de Seguridad Digital acorde 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.

Por otra parte, la Contaduría General de la Nación ha implementado el tratamiento y protección de los datos personales conforme a las disposiciones de la Resolución 1519 de 2020 de MinTIC que define los estándares y directrices para publicar la información institucional atendiendo los lineamientos de la Ley 1712 de 2014; y acoge en sus procesos el marco normativo y regulatorio de la entidad relacionada con la Seguridad y Privacidad de la Información (SPI).

De acuerdo con lo anterior, se 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 2023.

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 Política 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.

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: Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensibles o críticos para el cumplimiento de los objetivos de la CGN.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

CIGD – Sigla Comité Institucional de Gestión y Desempeño

Confidencialidad: Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

Control: Medida que modifica y mitiga el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: Acceso a la información cuando se requiere, teniendo en cuenta la privacidad.

GIT: Sigla Grupo Interno de Trabajo

Incidente de seguridad de la información: Un incidente de seguridad de la Información está indicado por un único evento o una serie de eventos de Seguridad de la Información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y de amenazar la seguridad de la información.

Integridad: Es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (impacto). (ISO/IEC 27000).

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

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

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. CONDICIONES GENERALES

La Alta Dirección promueve la seguridad y privacidad de la información (SPI), a través del cumplimiento de la política de privacidad y protección de los Datos; la Estrategia de Seguridad Digital; la gestión y tratamiento de riesgos; la implementación del SGSI; la adopción del marco regulatorio respectivo, así como la articulación de los procesos y la evaluación interna mediante el instrumento de autodiagnóstico del MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones, con la que se determinan los cambios a incorporar en el presente documento.

De igual forma, para llevar a cabo la preparación de plan de seguridad y privacidad de la información de la Contaduría General de la Nación se siguieron los lineamientos contenidos 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, la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la Información, Diseño de Controles en Entidades Pública, emitida por el Departamento Administrativo de la Función Pública – DAFP.

6. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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, Seguridad Digital de manera integral.
4. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
5. Generar la concientización para el uso y apropiación de la Seguridad y Privacidad de la Información como eje transversal de 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	CIGD	Aprobar el Plan SPI Tomar decisiones sobre los asuntos de la seguridad de la información
Rol Táctico	Oficial de Seguridad o quien haga sus veces.	Preparar y presentar el Plan SPI Asegurar la implementación de las políticas que se desarrollan para garantizar la confidencialidad, disponibilidad e integridad de la información en el marco del SGSI, la seguridad y privacidad la información y seguridad digital.
Rol Funcional	GIT Apoyo Informático	Ejecutar y hacer seguimiento al desarrollo del Plan SPI Informar sobre la gestión de la SPI
	Líderes de Procesos	Integrar los procesos institucionales a la gestión del SPI Ejecutar los controles a nivel de proceso para la seguridad y protección de los activos de información Promover las buenas prácticas de SPI

Funciones:

7.1. Comité de Seguridad de la Información

Las funciones del comité de Seguridad de la Información son asumidas por el Comité Institucional de gestión y desempeño mediante Resolución número 193 del 19 dejunio 2019.

7.2. 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.

7.3. Oficial de Seguridad o quien haga sus veces:

El rol del administrador del SGSI, 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 para la aplicación de controles en el sistema
- Realizar revisiones periódicas al SGSI y definir acciones conducentes a la mejora continua.
- Asegurar el cumplimiento de las políticas, normas, procedimientos, y demás lineamientos en materia de seguridad de la información.

7.4. Líderes de procesos:

El rol de los líderes de procesos en la ejecución del plan de revisión y seguimiento al SGSI, es fundamental dado que es el responsable 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

7.5. Coordinador de GIT de Apoyo Informático:

El GIT de apoyo informático y sus profesionales serán los responsables de loscontroles técnicos de seguridad de la información:

- Cierre de vulnerabilidades técnicas
- Seguimiento al cierre de vulnerabilidades técnicas
- Seguimiento de indicadores
- Seguimiento al cierre de eventos e incidentes de seguridad de la información
- Seguimiento del plan de tratamiento de riesgos de seguridad de la información del proceso Gestión Tics
- Establecer controles de seguridad de la información con el fin de mitigar los riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y/o servicios que presta el GIT de apoyo informático.

7.6. Funcionarios y Contratistas

- Implementar las normas, políticas y procedimientos definidos para el sostenimiento del SGSI.
- Mantener y garantizar 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 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

8. Plan de Implementación de la Seguridad y Privacidad de la Información

El Plan de implementación 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 (SPI) 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 SPI 2023 se presenta periódicamente al Comité Institucional de Gestión y Desempeño – CIGD, y documenta según los productos definidos.

A continuación, se presenta la programación de actividades que conforman el Plan SPI:

No.	Control	Actividades Por Ejecutar	Producto	Fecha inicial estimada	Fecha final estimada	Responsable
1	Diagnóstico MSPI	Realizar la actualización de la Matriz del MPSI	Matriz diagnóstico diligenciada	2/03/2023	31/05/2023	Gestión TICs
2	Política general de seguridad de la información	Revisar, ajustar y aprobar la Política de Seguridad de la información	Política de Seguridad de la Información Actualizada	2/05/2023	29/09/2023	Alta Dirección Planeación Integral Gestión TICs
3	Manual de seguridad de la información	Revisar, ajustar y aprobar el Manual de Seguridad de la Información.	Manual de Seguridad de la Información Actualizado	2/05/2023	29/09/2023	Gestión Tics Planeación Integral
4	Estrategia de Seguridad Digital	Revisar, ajustar y aprobar la Estrategia de Seguridad Digital	Estrategia de Seguridad Digital Actualizada	15/03/2023	29/09/2023	Gestión Tics Planeación Integral
		Realizar actividades para el fortalecimiento de capacidades a través de acuerdos con otras Entidades Nacionales en temas de Defensa y Seguridad Digital.	Actas de reuniones y/o acuerdos	15/03/2023	29/12/2023	Gestión Tics Planeación Integral, funcionarios de la CGN
5	Documentos del SGSI - Procedimiento	Revisar y ajustar los documentos de SGSI implementado en la	Procedimiento GTI-PR010, formatos, instructivos,	1/03/2023	31/10/2023	Gestión Tics Planeación

	de seguridad de la información y otros	CGN, de acuerdo con las actualizaciones definidas y aprobadas por el CIGD	políticas y flujogramas actualizados			Integral Todos los procesos del alcance del SGSI
6	Gestión de activos de Información	Validar, verificar, actualizar y aprobar el inventario de Activos de Información. Verificar, actualizar y aprobar el inventario de activos críticos, infraestructuras críticas y servicios esenciales.	Matriz de activos actualizada y aprobada	15/02/2023	31/06/2023	Gestión Tics Planeación Integral Todos los procesos del alcance del SGSI
7	Gestión de vulnerabilidades	Definir lineamientos para ejecutar las pruebas de vulnerabilidades Ejecución de pruebas de seguridad (análisis de vulnerabilidades) al menos una vez al año. Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades Realizar seguimiento al cierre de vulnerabilidad técnicas de acuerdo con su nivel de criticidad	Documentación gestión de vulnerabilidades y resultados de pruebas de vulnerabilidades	3/04/2023	29/12/2023	Gestión Tics

		** Verificar la ejecución del re- test de pruebas de seguridad ** Documentar las actualizaciones cuando ocurra un cambio importante en los activos de información producto del retest.				
8	Indicadores de seguridad de la información	Revisar, ajustar o formular, implementar y medir los indicadores del SGSI	Matriz con indicadores actualizados según periodicidad e informe del cumplimiento de las acciones correctivas en caso de que aplique	2/02/2023	31/12/2023	Planeación integral Gestión Tics
9	Gestión de riesgos (Identificación, Análisis y Evaluación de Riesgos)	Realizar la identificación, análisis y evaluación de riesgos de los activos de información	Matriz con la evaluación de riesgos incluidos los riesgos de los activos de información y seguridad digital.	1/06/2023	15/11/2023	Planeación integral Gestión Tics
		Realizar la identificación, análisis y evaluación de riesgos de los activos críticos, infraestructura crítica y servicios esenciales (entorno digital)		1/06/2023	15/11/2023	
		Realizar seguimiento trimestral al Mapa o Plan de Tratamiento de Riesgos de la CGN	Mapa o Plan de Tratamiento de Riesgos actualizado con soportes	8/05/2023	31/12/2023	

		Realizar valoración trimestral del riesgo residual para establecer las variaciones y/o ajustes de cada periodo cuando corresponda		8/05/2023	31/12/2023	Líderes de los procesos misionales de la CGN Gestión Tics
		Como parte del seguimiento se realiza la revisión y preparación de evidencias que respaldan la ejecución de las actividades de control establecidas en el Plan de Tratamiento de Riesgos		8/05/2023	31/12/2023	Planeación integral Gestión Tics
10	Plan de Continuidad de Negocio de TI y los Planes de Contingencia	Revisar, ajustar y aprobar el Plan de Continuidad de Negocio, sus Anexos y los Planes de Contingencia	Plan de Continuidad de Negocio de TI - Anexos y Plan de Contingencia actualizados	19/06/2023	29/09/2023	Gestión Tics
		Validar, verificar, actualizar la identificación y/o valoración de Riesgos de interrupción de la operación de la entidad según corresponda	Documentación de las pruebas realizadas	19/06/2023	31/10/2023	
		Realizar seguimiento y revisión de la ejecución de las pruebas del plan según Cronograma				

		Realizar seguimiento a la documentación y lecciones aprendidas de los resultados de las pruebas del Plan				
		Revisión de las acciones de mejora Identificadas en las pruebas del Plan				
11	Plan de comunicación, socialización y sensibilización	Elaborar y ejecutar el Plan de comunicación en temas relacionados con la seguridad de la información como complemento al PIC (Plan Institucional de Capacitación de la CGN	Plan de Sensibilización y toma de conciencia en temas relacionados con seguridad de la Información y Seguridad Digital	2/03/2023	29/12/2023	Gestión Tics
		Desarrollar un Plan de sensibilización y toma de conciencia sobre ciberseguridad para ejercer control y protección sobre los entornos digitales		2/03/2023	29/12/2023	Gestión Tics
		Realizar mínimo 2 sesiones de sensibilización en seguridad de la información en las jornadas de inducción y reinducción		6/03/2022	29/12/2023	Líderes de los procesos de la CGN, Talento humano, Gestión tics
						(Nota: Los lideres podrán realizar socializaciones internas de seguridad de la información

						cuando sea pertinente mas no es obligatorio)
		Hacer seguimiento a las evidencias de socialización del SGSI	Evidencias de socialización y sensibilización	2/01/2022	31/12/2022	Planeación integral
12	Auditoria (Internas – Externas)	Realizar auditorías internas y externas de la norma ISO 27001:2013	Informe de auditoría y Plan de Mejoramiento	2/03/2023	30/11/2023	Planeación Integral
		Realizar seguimiento al cierre de las no conformidades producto de las auditorías internas y externas al SGSI.				Todos los procesos del alcance del SGSI
		Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso				
13	Gestión de incidentes de seguridad	Gestionar los incidentes de Seguridad de la Información identificados	Formatos Registro de Incidentes y/o Eventos de Seguridad de la Información y Soportes gestión	1/01/2023	31/12/2023	Gestión Tics
		Socializar el procedimiento de respuesta de gestión de incidentes al GIT de Apoyo Informático	Presentación al GIT de Apoyo Informático	1/03/2023	31/08/2023	
		Realizar el seguimiento a la gestión de incidentes de seguridad de la	Presentación con los resultados de los incidentes ocurridos en tema de	1/01/2023	31/12/2023	

		información incluyendo cierre	seguridad y privacidad de la información			
		Realizar seguimiento a las lecciones aprendidas producto de la gestión del incidente				
		Realizar seguimiento de los reportes de eventos de seguridad de la información y tomar acciones.				
		Capacitar a los usuarios internos y partes interesadas sobre los boletines de CSIRT.	Evidencias de sensibilización	1/03/2023	29/12/2023	
14	Declaración de aplicabilidad - Anexo A	Revisión de los controles de la norma ISO 27001:2013	Declaración de aplicabilidad actualizada	2/03/2023	29/12/2023	Gestión Tics
		Actualizar declaración aplicando acciones y controles para la implementación del control				
		Seguimiento a la aplicación de los controles				

1. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
06-12-2018	V1	Elaboración del Plan
27-12-2019	V2	Actualización del Plan vigencia 2020
03-12-2020	V3	Actualización del Plan vigencia 2021
12-11-2021	V3	Actualización del Plan vigencia 2022
13-10-2022	V4	Actualización de las actividades numeral 6.
	V5	Actualización documento

Elaboró: Ing. Mónica Arias,
Revisó: Ing. Oralia Franco
Aprobó: Ing. Martha Zornosa Guerra