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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2026

DICIEMBRE DE 2025

CONTROL DE CAMBIOS

VERSIÓN	SECCIÓN	TIPO	FECHA DD/MM/AAAA	AUTOR	OBSERVACIONES
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
7.0	9	Actualización	30/11/2024	Git de Apoyo Informático Oficial de seguridad de la Información	Actualización de plan vigencia 2025
8.0	Todas	Actualización	10/12/2025	Git de Apoyo Informático Oficial de seguridad de la Información	Actualización de plan vigencia 2026 ajustado de acuerdo a lineamiento MINTIC Resolución 500 de 2021

Contenido

1. Introducción

La UAE Contaduría General de la Nación (CGN) presenta este plan en cumplimiento del Decreto 612 de 2018 – Plan de Acción y Planes Institucionales y el 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 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 y CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital.

2. Objetivo

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la CGN, mediante la implementación de actividades y controles que soporten la gestión de seguridad y privacidad de la información. Estas acciones se desarrollarán conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información, la norma NTC/ISO/IEC 27001:2022 y la Estrategia de Seguridad Digital, con el propósito de mitigar los riesgos a los que está expuesta la entidad y reducirlos a niveles aceptables definidos para la vigencia 2026.

2.1 Objetivos Específicos

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

3. Alcance

La gestión de la seguridad y privacidad de la información aplica a todos los procesos institucionales de la CGN y demás partes interesadas que comparten, utilizan, recolectan, procesan, intercambian o consultan 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 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.

EAOS: sigla de Equipo Operativo de Apoyo al Oficial de seguridad

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 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.

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

5. Documentos de Referencia

El Plan de Seguridad y privacidad de la Información se basa principalmente en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan de Seguridad y Privacidad de la Información como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Decreto 767 de 2022, "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital"

6. Roles y responsabilidades

Rol		Responsabilidad
Rol Estratégico	Comité Institucional de Gestión y Desempeño (CIGD)	- Aprobar el plan seguridad y privacidad de la información. - Tomar decisiones sobre los asuntos de la seguridad de la información y seguridad digital
Rol Táctico	Oficial de Seguridad y privacidad de la información	- Preparar, presentar y hacer seguimiento al plan seguridad y privacidad de la información. - Velar por la efectividad de las políticas de seguridad de la información y seguridad digital. - Gestionar los activos de Información

Rol		Responsabilidad
Rol Funcional y operativo	Equipo operativo de apoyo para el Oficial de Seguridad y Privacidad de la Información	- Informar sobre la gestión del plan de seguridad y privacidad de la información del proceso. - Implementar controles que ayuden a mitigar los riesgos de seguridad de la información y seguridad digital. - Velar por la protección de los activos de información del proceso - Realizar revisiones periódicas al Modelo de Seguridad y Privacidad de la Información (MSPI)
	Equipo Seguridad de la Información del GIT de Apoyo Informático	- Mejorar y evolucionar el Modelo de Seguridad y Privacidad de la Información - Definir y evolucionar la arquitectura de seguridad - Gestionar la seguridad informática en los servicios de TI y tecnológicos - Definir, gestionar y monitorear los riesgos de seguridad de información - Realizar y gestionar el plan de continuidad y contingencia de TI - Administrar y mantener los servicios de seguridad informática. - Promover, aplicar y mantener medidas de seguridad informática que protejan los activos tecnológicos contra amenazas vulnerabilidades. - Realizar proceso de análisis de vulnerabilidades, los respectivos planes de mitigación y seguimiento sobre los recursos tecnológicos.
	Funcionarios y colaboradores de la CGN	- Cumplir con las disposiciones establecidas en las políticas de seguridad de la información y seguridad digital. - Velar por la protección de los activos de información del proceso - Apoyar el mantenimiento y mejora continua del Sistema Integrado de Gestión Institucional (SGSI) en el área

7. Estado actual de la entidad respecto al sistema de gestión de seguridad de la información

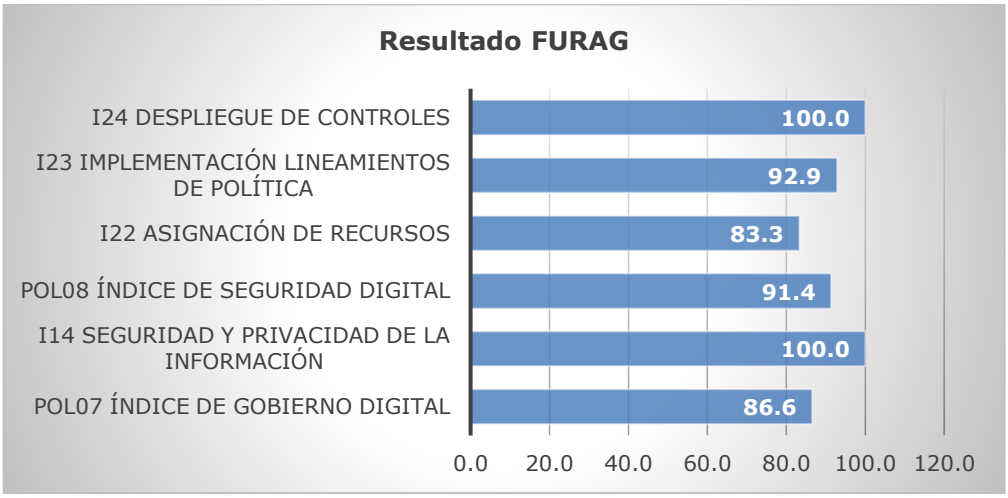
La CGN se encuentra en el proceso de transición a la Norma Técnica Colombiana ISO/IEC 27001:2022, y ha adoptado e implementado el Modelo de Seguridad y

Privacidad de la información, e identificado a través de la herramienta de autodiagnóstico (Análisis GAP) dispuesta por MinTIC, el estado actual de la entidad respecto a la Seguridad y privacidadde la Información, la cual se gestiona y monitorea a través del ciclo PHVA; Actualmente la entidad se encuentra en un nivel de madurez **Optimizado**, esto de acuerdo con los criterios que tiene la herramienta. Este nivel de madurez se determina a través de la implementación de los controles, los cuales se monitorean, se miden y se toman acciones permanentemente en determinados procesos que no están funcionando eficientemente o necesitan acción de mejora y seguimiento.

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**Nivel de Madurez**
A.5	CONTROLES ORGANIZACIONALES	91	100	**OPTIMIZADO**
A.6	CONTROLES DE PERSONAS	98	100	**OPTIMIZADO**
A.7	CONTROLES FÍSICOS	97	100	**OPTIMIZADO**
A.8	CONTROLES TECNOLÓGICOS	89	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**94**	**100**	**OPTIMIZADO**

Fuente: Herramienta de autodiagnóstico de MINTIC, vigencia 2025

Resultado de desempeño institucional – FURAG 2024

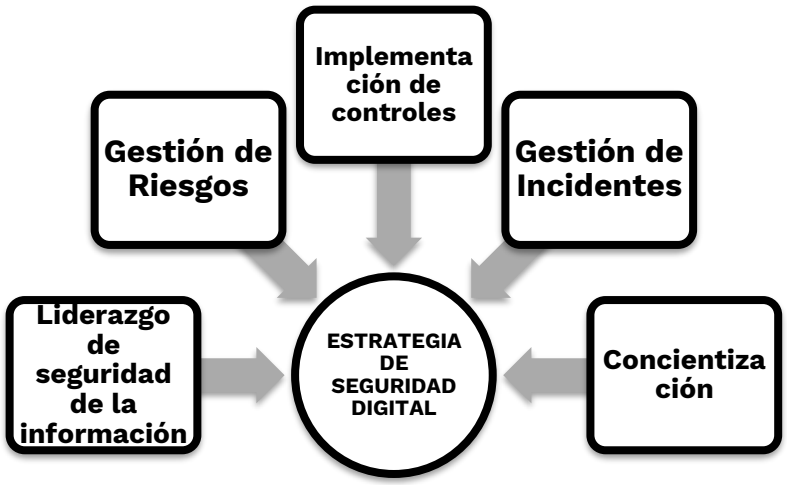


Fuente: Autodiagnóstico FURAG 2024

8. Estrategia de seguridad digital

La entidad define la estrategia de seguridad digital basada en los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información del MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad de la información.

Por lo anterior, la entidad define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



Fuente: Ministerio de Tecnologías de La Información y Las Comunicaciones, producto tipo Plan estratégico de seguridad de la información

El estado de implementación del SGSI con que cuenta la entidad garantiza la seguridad de la información a través del establecimiento de políticas, procedimientos y controles para la protección de la información institucional.

Se tienen implementados indicadores que permiten medir y monitorear los objetivos del Sistema de Gestión de Seguridad de la Información - SGSI.

El SGSI está integrado con el Modelo de Seguridad y Privacidad de la información y se articula con los otros sistemas de gestión de la entidad.

8.1 Descripción de las estrategias específicas

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MSPI y la resolución 500 de 2021:

ESTRATEGIA	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el MSPI a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la entidad.

Fuente: Ministerio de Tecnologías de La Información y Las Comunicaciones, producto tipo Plan estratégico de seguridad de la información

9. Portafolio de actividades:

Para cada estrategia específica, la CGN define los siguientes estrategías y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del SGSI:

No	Estrategia	Tema	Actividades Por Ejecutar	Producto	Tiempo estimado	Responsable	Avance 2026
1	Liderazgo de Seguridad de la Información	Diagnóstico MSPI (Declaración de Aplicabilidad)	Revisión y actualización del MSPI mediante la declaración de aplicabilidad	Declaración de aplicabilidad actualizada	1er semestre	Gestión TICs	
2		Manual del SGSI	Realizar la revisión y actualización del Manual del SGSI y Políticas de Seguridad de la Información	Manual del SGSI y políticas actualizadas.		Alta Dirección Gestión TICs EAOS - Equipo Operativo de Apoyo al Oficial de seguridad Planeación Integral	
3	Gestión de riesgos	Riesgos de Seguridad de Información y Seguridad digital	Revisar, valorar y clasificar los riesgos asociados a los activos de información	Matriz de riesgos de seguridad de la información y seguridad digital actualizada	1er Semestre	Planeación Integral	
4			Revisar y actualizar el tratamiento de riesgos de seguridad de la información y seguridad digital			Gestión TICs	
5			Realizar seguimiento al tratamiento y control de acciones de los riesgos de seguridad de la información y seguridad digital			Todos los procesos del alcance del SGSI	

No	Estrategia	Tema	Actividades Por Ejecutar	Producto	Tiempo estimado	Responsable	Avance 2026
6	Concientización	Concientización de Seguridad de la Información y Seguridad Digital	Realizar actividades de sensibilización al personal de la CGN	Plan y evidencias de las actividades desarrolladas	1er y 2do Semestre	Proceso Gestión TICs	
7	Implementación de controles	Documentos del SGSI	Revisar, actualizar y gestionar los documentos de SGSI	Documentos del SGSI actualizados	2do Semestre	Gestión Tics Planeación Integral Todos los procesos del alcance del SGSI EAOS	
8	Gestión de incidentes	Eventos e incidentes de Seguridad de la Información y Seguridad Digital	Realizar Gestión de Incidentes de seguridad de la información.	Indicador de gestión de incidentes	1er y 2do Semestre	Proceso Gestión TICs Oficial de seguridad EAOS, CIGD	
9			Sensibilizar al personal en la gestión de incidentes de seguridad de la información.	Registro de sesiones de sensibilización desarrolladas.		Proceso Gestión TICs	

Fuente: Elaboración Propia

10. Análisis Presupuestal

El presupuesto aproximado presentado a la Alta Dirección y con viabilidad para la vigencia 2026 según las actividades establecidas es el siguiente:

Proyecto de inversión del GIT de Apoyo Informático "Fortalecimiento de la plataforma tecnológica para la prestación de los servicios de la CGN Nacional"

Actividad: Actualizar la estrategia de seguridad de la información de la CGN

Objeto	2025	Valor proyectado 2026	Observaciones
Renovación de licencia de la SUITE DE SEGURIDAD ANTIVIRUS - ESET PROTECT ON PREMISE A ESET PROTECT ELITE ON CLOUD, para la plataforma tecnológica de la U.A.E Contaduría General de la Nación, por dos (2) años para trescientos (300) endpoint y renovación del servicio de análisis de vulnerabilidades a una Herramienta de Vulnerabilidades 7x24 para ciento veinte (120) endpoint, administrada por la U.A.E Contaduría General de la Nación	124.900.000		Va por dos años hasta noviembre de 2027
Renovación de la garantía, soporte y mantenimiento para los siguientes equipos: Dos (2) Firewall Fortigate 601E, un (1) FortiAnalyzer 400E, Cinco (5) Access Point FortiAP U231F ubicados en la ciudad de Bogotá, Un (1) Firewall Fortigate 100F ubicado en la ciudad de Medellín.	269.781.330	290.000.000	Vence 27/03/2026 y requiere renovar
Adquisición, instalación y puesta en funcionamiento de dos (2) switch para datacenter y un (1) firewall de aplicaciones web para la red de datos de la CGN	535.947.428		Va por dos años el soporte y garantía
Contratación de profesional especializado	56.458.500	63.525.000	11 meses
TOTAL	406.458.500	**353.525.000**	

11. Seguimiento al Plan de Seguridad y Privacidad de la Información

El diagnóstico de la gestión del Plan de Seguridad de la Información 2025 se presenta a continuación y se incluyen las acciones de mejora para seguir con su cumplimiento:

No	Estrategia	Tema	Actividades Por Ejecutar	Producto	Tiempo estimado	Responsable	Avance 2025
1	Liderazgo de Seguridad de la Información	Diagnóstico MSPI	Realizar actualización de Matriz del MSPI	Matriz de diagnóstico actualizada.	2do Semestre	Proceso Gestión TICs	Actualizado en la declaración de aplicabilidad
2		Declaración de Aplicabilidad	Revisión y actualización si es necesario de la declaración de aplicabilidad	Declaración de aplicabilidad actualizada		Proceso Gestión TICs	Actualizado
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	Se actualizan los documentos: Política General de Seguridad de la Información y seguridad digital, Políticas de Seguridad de la Información y Seguridad Digital y Manual del

No	Estrategia	Tema	Actividades Por Ejecutar	Producto	Tiempo estimado	Responsable	Avance 2025
							SGSI
4	Gestión de activos	Activos de información	Revisar, identificar, actualizar y aprobar el 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	Actualizado
5	Gestión de riesgos	Riesgos de Seguridad de Información y Seguridad digital	Revisar, valorar y clasificar los riesgos asociados a los activos de información	Matriz de riesgos de seguridad de la información y seguridad digital actualizada	1er Semestre	Planeación Integral	Actualizado a la versión 6 del DAFP
6			Revisar y actualizar el tratamiento de riesgos de seguridad de la información y seguridad digital			Gestión Tics	
7			Realizar seguimiento al tratamiento y control de acciones de los riesgos de seguridad de la información y seguridad digital			Todos los procesos del alcance del SGSI	
8	Gestión de controles	Documentos del SGSI	Revisar, actualizar y gestionar los documentos de SGSI	Documentos del SGSI actualizados	2do Semestre	Gestión Tics Planeación Integral Todos los procesos del alcance del SGSI Secretaría General	Actualización de procedimientos, formatos, guías, instructivos **Plan de mejora:** se continuará con actualización de otros documentos del SGSI
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	Pruebas realizadas retest diciembre 2024 Hardware y retest julio de 2025 Software
10			Realizar seguimiento, cierre y retest de las vulnerabilidades.				En proceso de cierre de vulnerabilidades
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 Planeación Integral Secretaría General	Actualizado
12			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.		Proceso Gestión TICs Secretaría General	Realizado

No	Estrategia	Tema	Actividades Por Ejecutar	Producto	Tiempo estimado	Responsable	Avance 2025
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	Plan de comunicaciones y sensibilización seguridad de la información y seguridad digital en ejecución

Fuente: Elaboración propia

12. Bibliografía:

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: Martha Zornosa Guerra
Revisó y aprobó: Anuar Vargas Calderón
Aprobó: Freddy Castaño Pineda