MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	SEGURIDAD DE LA INFORMACIÓN		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/11/2024	GTI-MAN01	02	**1** de **24**

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

OCTUBRE DE 2024

CONTROL DE CAMBIOS

VERSIÓN	SECCIÓN	TIPO	FECHA (DD/MM/ AAAA)	AUTOR	OBSERVACIONES
1.0	Todas	Creación	15/07/2024	GIT de Apoyo Informático	Creación del documento Aprobado el 30/10/2024 en CIGD

CONTENIDO

1. INTRODUCCIÓN

La Contaduría General de la Nación, en adelante CGN, se compromete a desarrollar una gestión segura y proporcionar un ambiente adecuado para la óptima operación de los activos de información y la plataforma tecnológica que respalda los procesos, garantizando la confidencialidad, disponibilidad e integridad de la información a través de prácticas sólidas de seguridad digital.

El objetivo de este manual es presentar las directrices y lineamientos definidos para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, en adelante SGSI, acorde con los requisitos de la Norma NTC-ISO-IEC 27001.

Para efectos de este documento, se entiende por SGSI como el conjunto de normas, estructura de organización, programas, políticas, protocolos, lineamientos, espacios físicos, información documentada y recursos humanos que se destinan para el desarrollo de las operaciones de los procesos y áreas establecidas dentro de la CGN.

2. ALCANCE DE ESTE DOCUMENTO

Describir de forma general el cumplimiento de los requisitos establecidos en los numerales 4 al 10 de la Norma NTC-ISO-IEC 27001:

4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

3. TÉRMINOS Y DEFINICIONES:

Las definiciones relacionadas con Seguridad de la Información, Ciberseguridad y Protección de Datos Personales se encuentran unificadas en el documento GTI-MAN02 Manual de Términos y Definiciones de Seguridad de la Información y Seguridad Digital.

4. CONTEXTO DE LA ORGANIZACIÓN

El contexto de la organización lo define la alta dirección, que es responsable del Plan Estratégico Institucional (PEI), el cual busca el logro de los objetivos estratégicos propuestos en su misión y el alcance de su visión. Así mismo, este contexto es tenido en cuenta en la planificación de los Sistemas de Gestión Institucional.

4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO

En cumplimiento del numeral 4.1 de la norma NTC-ISO/IEC 27001, la CGN identificó las cuestiones externas e internas que son pertinentes para su propósito mediante la aplicación de una Matriz DOFA, en la cual, además, se destaca el análisis de las estrategias F-A: disminuir las amenazas aprovechando las fortalezas; y las estrategias D-A: minimizar las debilidades y evitar las amenazas.

Más información en: https://www.contaduria.gov.co/nuestra-entidad.

4.1.1 Historia

El artículo 354 de la Constitución Política de Colombia de 1991 creó la figura de Contador General de la Nación y le confirió las funciones de llevar la contabilidad general de la Nación y consolidar esta con la de sus entidades descentralizadas territorialmente o por servicios, así como uniformar, centralizar y consolidar la contabilidad pública; elaborar el balance general; y determinar las normas contables que deben regir en el país.

Posteriormente, con el Decreto 85 de 1995 se creó la Dirección General de Contabilidad Pública (DGCP), a cargo del Contador General de la Nación, como una dependencia del Ministerio de Hacienda y Crédito Público. En este mismo año, mediante la Resolución 4444, fue expedido el primer Plan General de Contabilidad Pública. Este plan fue el instrumento de regulación con base en el cual las entidades públicas presentaron el primer balance general bajo el principio de devengo a 31 de diciembre de 1995.

La Ley 298 de 1996 desarrolló el artículo 354 de la Constitución Política y creó la Contaduría General de la Nación como una Unidad Administrativa Especial con personería jurídica y autonomía presupuestal, técnica y administrativa.

Más información en: https://www.contaduria.gov.co/resena-historica.

4.1.2 Misión

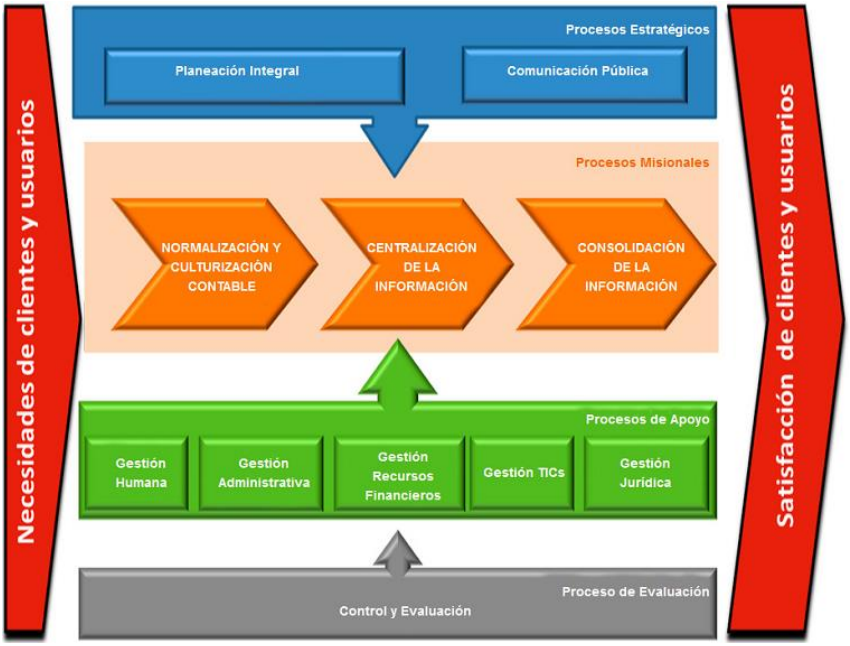
Somos el órgano rector de la contabilidad pública en Colombia, con autoridad doctrinaria en la materia, que normaliza, centraliza y consolida la contabilidad del sector público, para elaborar el Balance General de la Nación y de la Hacienda Pública, así como otros informes contables, útiles para la toma de decisiones, la rendición de cuentas y el control de las entidades públicas, los ciudadanos y demás grupos de valor.

4.1.3 Visión

Seremos reconocidos como una entidad pilar del Sistema de Gestión Financiera Pública, que innova en la provisión de la información contable pública relevante y confiable para la transparencia, eficiencia y sustentabilidad social y ambiental del sector público colombiano, orientada a la creación de valor público para la sociedad.

4.1.4 Mapa de procesos y objetivos

El mapa de procesos de la CGN está conformado por cuatro grupos: estratégicos, misionales, de apoyo y evaluación:



El detalle de los objetivos de cada proceso se puede consultar en: https://www.contaduria.gov.co/web/guest/mapa-de-procesos-y-objetivos.

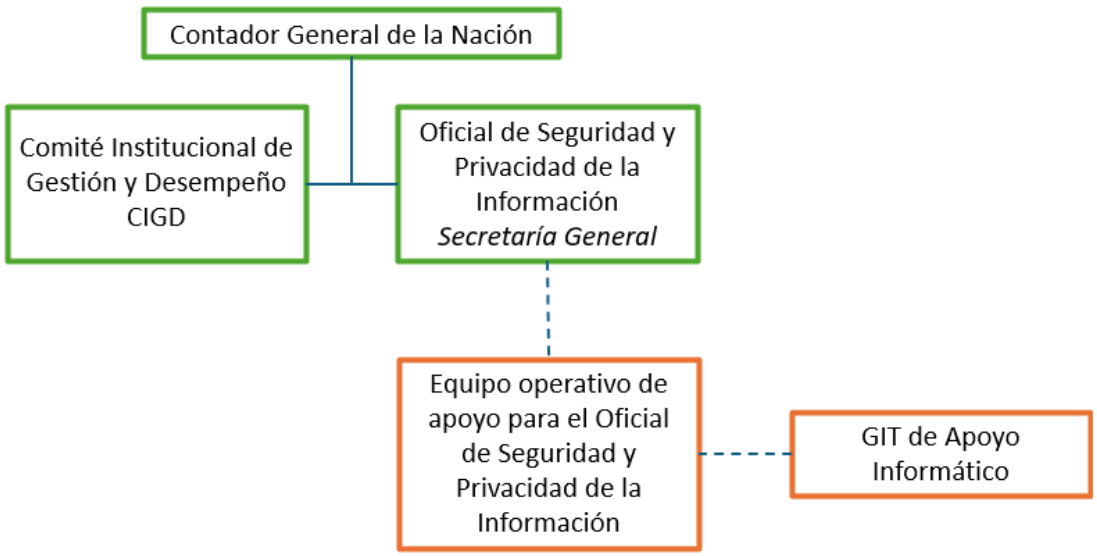
4.1.5 Estructura de Roles para el Gobierno de Seguridad de la Información

Mediante la Resolución 193 del 19 de junio de 2019 se crea el Comité Institucional de Gestión y Desempeño como órgano de asesoría y coordinación para definir estrategias y políticas orientadas a la determinación y mejoramiento continuo, entre otros, del SGSI.

Así mismo, mediante la Resolución 383 del 15 de noviembre de 2023 se designa al Secretario General como Oficial de Seguridad y Privacidad de la Información.

De igual manera, mediante la Resolución 246 del 22 de julio de 2024 se crea el equipo operativo de apoyo para el Oficial de Seguridad y Privacidad de la Información.

La estructura de roles para el gobierno de seguridad de la información es la siguiente:



Fuente: Elaboración propia

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

La CGN identificó las partes interesadas internas y externas, así como sus necesidades y expectativas en cuanto a seguridad de la información, las cuales se detallan en el siguiente enlace: https://www.contaduria.gov.co/documents/20127/35671/Matriz+Partes+interesadas.xlsx.

4.3 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) certifica que el SGSI ha sido auditado y aprobado con respecto a los requisitos especificados en la Norma ISO/IEC 27001 mediante el certificado CO-SI-CER660642 otorgado el 2019-01-11, y es aplicable al siguiente alcance: "Determinación de las políticas, principios y normas de contabilidad para el sector público colombiano. Unificación, centralización y consolidación de la información contable y elaboración del balance general Consolidado de la nación".

4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con lo anterior, la CGN establece, implementa, mantiene y mejora de manera continua el SGSI, de acuerdo con los requisitos de la norma internacional ISO/IEC 27001 y el Anexo A de controles, presentados en el desarrollo del presente documento.

5. LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO

La alta dirección de la CGN demuestra su compromiso, liderazgo y apoyo con el SGSI llevando a cabo las actividades descritas en el numeral 5.2 de este documento. De igual forma, se instituye un Comité Institucional de Gestión y Desempeño (CIGD), en el que se presentan mensualmente los avances en las actividades pertinentes a seguridad de la información y se lleva a cabo la revisión del SGSI de acuerdo con lo establecido en el documento *PI-PRC17 Revisión por la Dirección* y en las funciones del CIGD.

5.2 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La CGN, como órgano rector de la contabilidad pública en Colombia, con autoridad doctrinaria en la materia, que normaliza, centraliza y consolida la contabilidad del sector público, para elaborar el Balance General de la Nación y de la Hacienda Pública, reconoce la información como un activo fundamental que debe ser protegido frente a amenazas internas o externas que puedan comprometer la confidencialidad, integridad y disponibilidad de esta.

Por lo anterior, la CGN establece estrategias y controles lógicos, físicos y digitales en el marco de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001, para asegurar la infraestructura crítica que soporta los procesos misionales, garantizando la disposición de recursos requeridos y adoptando un enfoque basado en la gestión de riesgos de seguridad de la información, la gestión de incidentes de seguridad de la información y la mejora continua del SGSI.

En cumplimiento de lo manifestado, la CGN se compromete a garantizar, verificar y cumplir todos los requisitos legales, reglamentarios, regulatorios, contractuales y de gestión documental, orientado a la mejora continua, eficacia del SGSI, y al cumplimiento de los objetivos de seguridad de la información establecidos por la Alta Dirección.

5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES

La estructura de roles para el gobierno de seguridad de la información se presenta en el numeral 4.1.5 de este documento. No obstante, el detalle de roles, responsabilidades y autoridades está condensado en varias resoluciones oficiales, que se citan a continuación:

5.3.1 Comité Institucional de Gestión y Desempeño (CIGD) Comité de Seguridad de la Información

Resolución 193 de 2019

Artículo 6. Composición:

- Contador General de la Nación
- Líder del proceso de Planeación Integral
- Líder del proceso de Comunicación Pública
- Líder del proceso de Normalización y Culturización Contable

- Líder del proceso de Centralización de la Información
- Líder del proceso de Consolidación de la Información
- Líder del proceso de Gestión Humana
- Líder del proceso de Gestión Administrativa
- Líder del proceso de Gestión Recursos Financieros
- Líder del proceso de Gestión TICs
- Líder del proceso de Gestión Jurídica
- Líder del proceso de Control y Evaluación (con voz, pero sin voto)
- Asesor 1020-13

Artículo 7. Funciones del Comité:

- Establecer las políticas y lineamientos para planear, organizar, dirigir, controlar y coordinar las actividades relacionadas con la Política de Seguridad y/o Gobierno Digital, con el fin de garantizar la aplicación de los principios y directrices establecidas en las normas que regulan la materia.
- Revisar los lineamientos técnicos y operativos para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), con base en el Manual y la Política de Gobierno Digital.
- Designar el responsable de seguridad digital y del SGSI de la CGN.
- Asignar el rol de Oficial de Seguridad y Privacidad de la Información, en cumplimiento de los lineamientos establecidos en la Norma NTC ISO-IEC 27001.
- Soportar la administración y desarrollo de iniciativas de seguridad de la información a través de compromisos y de la disponibilidad de recursos, así como la formulación, actualización y divulgación de la política de seguridad de la información al interior de la entidad.
- Generar recomendaciones para la formulación, adecuación y aprobación de políticas, planes, programas y proyectos en materia de seguridad de la información y controles específicos de seguridad para la implementación de nuevos servicios
- Revisar el manejo de la gestión de incidentes de seguridad en busca de la mejora continua, basados en experiencias propias y de otras entidades.
- Con base en los resultados del análisis de riesgos de los activos de información, revisar y aprobar el plan de mitigación del riesgo que contribuya al mejoramiento continuo del SGSI.
- Realizar revisiones al SGSI periódicamente y, según los resultados de esta revisión, definir las acciones a seguir.

- Consultar jurídicamente las medidas a implantar, recurriendo a los entes encargados de los temas jurídicos para validar las medidas necesarias cuando un incidente de seguridad lo requiera.
- Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados con la seguridad de la información dentro de la CGN.

Artículo 13. Sesiones:

El CIGD se reunirá de forma ordinaria cada mes, o de forma extraordinaria cuando el presidente o los integrantes del CIGD lo soliciten, acorde con las circunstancias que así lo ameriten.

5.3.2 Secretario General (Oficial de Seguridad y Privacidad de la Información)

Resolución 383 de 2023

Artículo 3. Designación y responsabilidad del Oficial de Seguridad y Privacidad de la Información:

El Oficial de Seguridad y Privacidad de la Información será el Secretario General o quien haga sus veces. El Oficial de Seguridad y Privacidad de la Información será el responsable de liderar todo el ciclo PHVA (Planear, Hacer, Verificar y Actuar) del Modelo de Seguridad y Privacidad de la Información (MSPI), no obstante, para la correcta ejecución de sus funciones o decisiones se requiere del GIT de Apoyo Informático.

Artículo 4. Funciones del Oficial de Seguridad y Privacidad de la Información:

- Liderar el cumplimiento al ciclo PHVA del MSPI.
- Definir y elaborar documentos que sean de su competencia para la operación del MSPI, actualizar y definir políticas, normas, procedimientos y estándares, manuales, metodologías del MSPI que sean de su competencia, así como apoyar otros procesos que requieran brindar lineamientos relacionados con seguridad de la información.
- Realizar, proponer y exponer riesgos cibernéticos en materia de seguridad y privacidad de la información de acuerdo con los proyectos y/o procesos de la entidad.

- Brindar acompañamiento a los procesos de la entidad en la identificación, clasificación de activos de información y tratamiento de riesgos de seguridad digital, que puedan comprometer las operaciones de la CGN y pueda amenazar la seguridad de la información de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad.
- Definir e implementar actividades de divulgación, campañas o capacitaciones de socialización sobre seguridad y privacidad de la información para servidores públicos, contratistas y partes interesadas que consulten o reciban servicios de la CGN.
- Apoyar, proponer y hacer seguimiento a los procesos en los planes de mejoramiento para dar cumplimiento a las recomendaciones en materia de seguridad y privacidad de la información.
- Definir, implementar y aplicar el procedimiento de gestión de incidentes de seguridad y privacidad de la información en la entidad, con el fin de detectar, contener, reportar, evaluar, responder, tratar e identificar las lecciones aprendidas de incidentes de seguridad y privacidad de la información.
- Hacer seguimiento y proponer los controles necesarios a los procesos en la implementación de las políticas de seguridad y privacidad de la información en la CGN.
- Adelantar acciones de articulación con la Coordinación del GIT de Apoyo Informático de la entidad sobre seguridad de la información y seguridad digital, para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.
- Efectuar acompañamiento y dar recomendaciones a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos de seguridad y privacidad de la información.
- Realizar el análisis de riesgos a las aplicaciones y sistemas de información de uso de la CGN.
- Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad de las funciones misionales de la entidad.
- Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad y privacidad de la información.
- Impartir lineamientos y hacer seguimiento para controlar el acceso a los sistemas de información y la modificación de privilegios.
- Promover la formación, educación y el entrenamiento en seguridad y privacidad de la información.

- Recibir capacitación en el tema de seguridad y privacidad de la información; mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes con el fin de socializar y divulgar al interior de la entidad; adoptar mejores prácticas de seguridad de la información en la plataforma tecnológica y sistemas de información. Adicionalmente, replicar a todas las partes interesadas de la CGN los nuevos conocimientos aprendidos en el uso y apropiación de seguridad de la información.
- Realizar estudios de penetración y pruebas de vulnerabilidades en todos los ambientes (desarrollo, pruebas, producción y contingencia) a los servidores, equipos de comunicación, seguridad y sistemas de información, resultado de los procesos de gestión de sistemas de información y gestión de configuración y activos de los servicios de Tecnologías de la Información (TI). De igual forma, recomendar controles o planes de tratamiento para la mitigación de las vulnerabilidades.
- Informar al CIGD de la entidad cuando se presenten violaciones a los controles de seguridad de bases de datos que contengan datos personales y existan riesgos en la administración de la información de los titulares, para evaluar la pertinencia de informar a la Superintendencia de Industria y Comercio (SIC).
- Coordinar y apoyar las auditorías internas y externas al SGSI enmarcadas en las responsabilidades de la segunda línea de defensa de acuerdo con el Modelo Estándar de Control Interno, sin que en ningún caso pueda auditar su propio proceso.
- Realizar seguimiento a la implementación de las recomendaciones en materia de seguridad de la información que hayan resultado de cada auditoría.
- Realizar el monitoreo del cumplimiento de las políticas y procedimientos que se restablezcan en materia de seguridad de la información, sin perjuicio de aquellas tareas que realizan las autoridades de control.
- Estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad en materia de seguridad y privacidad de la información, de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad.
- Evaluar las medidas de seguridad, privacidad y circulación restringida en transferencia de información a otras entidades para garantizar la autenticidad, integridad, disponibilidad, confidencialidad, acceso y circulación restringida de la información,

de conformidad con lo estipulado en el habilitador transversal de seguridad de la información de la Política de Gobierno Digital.

- Reportar a la Oficina de Control Disciplinario Interno las presuntas violaciones de los servidores públicos al cumplimiento de las políticas del Manual de Seguridad y Privacidad de la Información, que generaron un incidente que afectó la integridad, la disponibilidad o la confidencialidad de la información de la entidad, para su respectiva investigación y acciones a las que haya lugar.
- Aplicar las demás consideraciones que a juicio de la Nación y la entidad contribuyan a elevar sus estándares de seguridad y privacidad de la información.

5.3.3 Equipo operativo de apoyo para el Oficial de Seguridad y Privacidad de la Información

Resolución 246 del 2024

Artículo 1. Integrantes:

- Subcontador(a) General y de Investigación o su delegado(a)
- Subcontador(a) de Centralización de la Información o su delegado(a)
- Subcontador(a) de Consolidación de la Información o su delegado(a)
- Coordinador(a) del GIT de Jurídica o su delegado(a)
- Coordinador(a) del GIT de Apoyo Informático o su delegado(a)
- Coordinador(a) del GIT Logístico de Capacitación y Prensa o su delegado(a)
- Coordinador(a) del GIT de Planeación o su delegado(a)
- Secretario(a) General o su delegado(a)

Artículo 3. Funciones:

- Recomendar al Oficial de Seguridad y Privacidad de la Información la adopción de políticas, planes, lineamientos, metodologías, estrategias, medidas o controles de mitigación o prevención de incidentes de seguridad y su mecanismo de evaluación.
- Notificar al Oficial de Seguridad y Privacidad de la Información los incidentes de seguridad de la información que se registren en los sistemas de información de la Contaduría General de la Nación.
- Informar al Oficial de Seguridad y Privacidad de la Información los riesgos cibernéticos de seguridad de la información que se identifiquen en los sistemas de información de la Contaduría General

de la Nación; previa revisión de los diagnósticos del estado de la seguridad y privacidad de la información.

- Recomendar la aplicación de políticas y procedimientos de seguridad de la información en la operación de los procesos que lo requieran por su especificidad.
- Evaluar y recomendar la implementación de controles específicos de seguridad y privacidad de la información para los sistemas o servicios que utilicen la plataforma tecnológica de la CGN, sean preexistentes o nuevos.
- Realizar revisiones periódicas al Modelo de Seguridad y Privacidad de la Información (MSPI) (por lo menos una vez al año) y, según los resultados de esta revisión, definir las acciones pertinentes.
- Proponer acciones para gestionar la consecución y asignación de recursos, económicos y tecnológicos que garanticen la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Informar el avance de actividades del plan de seguridad y privacidad de la información y seguridad digital.
- Brindar apoyo a los procesos de la entidad en la identificación, clasificación y valoración de activos de información y tratamiento de riesgos de seguridad de la información y seguridad digital.
- Informar sobre la aplicación y desarrollo de los planes de contingencia y continuidad de negocio.
- Proponer y coordinar actividades del plan de formación y sensibilización de la entidad en los temas de seguridad de la información y evaluar su resultado cuando aplique.
- Las demás funciones inherentes a la naturaleza del equipo operativo de apoyo y las que le sean propias de acuerdo con la normativa sobreviniente.

Artículo 5. Obligaciones de los integrantes:

- Asistir a las reuniones que sean convocados.
- Suscribir las actas de cada sesión.
- Suscribir las comunicaciones que, en ejercicio de sus funciones, expida el equipo operativo de apoyo.
- Las demás funciones que establezca la ley.

Artículo 6. Reuniones y funcionamiento:

Se reunirá de forma ordinaria como mínimo una (1) vez cada dos meses cuando existan temas que deban ser abordados por este, previa convocatoria de la Secretaría Técnica del equipo. También se podrá reunir de forma extraordinaria por solicitud de los integrantes y previa citación de la Secretaría Técnica.

5.3.4 GIT de Apoyo Informático – Coordinación GIT

El GIT de Apoyo Informático vela por la correcta utilización de todos los recursos tecnológicos y comunicaciones de la Contaduría, como lo son: equipos de cómputo, sistemas de información, aplicativos, portales web, redes, procesamiento de datos e información y canales de comunicación. El GIT, como administrador de la infraestructura tecnológica, promueve la adecuada gestión de la seguridad de la información procesada, transferida y almacenada en los sistemas y en los servicios de Tecnologías de la Información.

5.3.4 Planta global

Resolución 371 del 2023. Manual Específico de Funciones y Competencias Laborales de la UAE Contaduría General de la Nación (página 44 en adelante)

- Apoyar el mantenimiento y mejora continua del Sistema Integrado de Gestión Institucional (SGSI) en el área, con el fin de garantizar el cumplimiento de los requisitos establecidos.
- Cumplir con las disposiciones establecidas en las normas NTC ISO 9001, NTC ISO 14001, NTC ISO 45001 e ISO 27001 en sus versiones vigentes, así como direccionar a su equipo de trabajo en el cumplimiento de estas.

Más información en:
https://www.contaduria.gov.co/documents/20127/5793072/Res+371+del+09+de+noviembre+de+2023+ajuste+manual+de+funciones.pdf/

6. PLANIFICACIÓN

6.1 ACCIONES PARA TRATAR EL RIESGO Y OPORTUNIDADES

La CGN, mediante el documento *Políticas de Administración del Riesgo*, establece las directrices para la gestión de riesgo, denotando el grado de compromiso de la entidad frente al cumplimiento de los objetivos estratégicos y del Plan de Acción Institucional, direccionando a los procesos a asumir un pensamiento basado en riesgos, que permita anticiparse, disminuir y contrarrestar el impacto de eventos inesperados. Para lograr lo anterior, se adopta el documento Excel *Plan de Tratamiento de Riesgos de Seguridad de la Información y Seguridad Digital*, que contiene el mapa de tratamiento de riesgos.

Esta política toma como base el Modelo Integrado de Planeación y Gestión (MIPG), la Norma Técnica Colombiana NTC-ISO 31000:2018, el Decreto 2641 de 2012, la Metodología General Ajustada (MGA WEB) y la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas* expedida por la Presidencia de la República, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Departamento Administrativo de la Función Pública y el Departamento Nacional de Planeación.

Más información en: https://www.contaduria.gov.co/riesgos

6.1.1 Oportunidades de seguridad de la información

El documento Excel *Plan de Tratamiento de Riesgos de Seguridad de la Información y Seguridad Digital*, que contiene el mapa de tratamiento de riesgos, considera el tratamiento de oportunidades.

Más información en: https://www.contaduria.gov.co/riesgos

6.1.2 Evaluación de riesgos de la seguridad de la información

El documento *Política de Administración del Riesgo* establece el lineamiento de evaluación de riesgos de la seguridad de la información, mediante los criterios de calificación del impacto definidos. Además, el documento *Mapa de Riesgos Institucional* permite la aplicación de los lineamientos de valoración de riesgos.

Más información en: https://www.contaduria.gov.co/riesgos

6.1.3 Tratamiento de riesgos de la seguridad de la información

El documento *Política de Administración del Riesgo* establece el lineamiento de tratamiento de riesgos de la seguridad de la información. De acuerdo con la evaluación del impacto, los riesgos se pueden aceptar, evitar, compartir o reducir.

Más información en: https://www.contaduria.gov.co/riesgos

La CGN, al determinar reducir el riesgo, compara los riesgos identificados con la lista de controles del Anexo A y verifica que no se omitan controles necesarios mediante el documento de declaración de aplicabilidad.

Más información en:https://www.contaduria.gov.co/web/intranet/sistema-de-gestion-de-seguridad-de-la-informacion

6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANIFICACIÓN

Para dar cumplimiento a la Política de Seguridad de la Información, la CGN define los siguientes objetivos de seguridad de la información:

- Proteger la información recibida y generada por la CGN en sus procesos, mediante la implementación de controles de conformidad con la norma NTC ISO/IEC 27001.
- Asegurar la protección de los activos informáticos de apoyo en los procesos misionales.
- Identificar y dar cumplimiento a los requisitos legales y regulatorios, así como a las obligaciones contractuales de la Contaduría General de la Nación.
- Gestionar los riesgos de seguridad de la información de acuerdo con las directrices de la entidad, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.
- Capacitar y sensibilizar al personal en temas relacionados con seguridad de la información, buscando un aumento progresivo en la cultura de seguridad al interior de la entidad, reflejado en el nivel de cumplimiento de políticas y procedimientos; y, además, en el reporte de eventos e incidentes de seguridad.

Más información en: https://www.contaduria.gov.co/objetivos-del-sistema-integrado-de-gestion-institucional

7. SOPORTE

7.1 RECURSOS

Los procesos de la CGN que contribuyen a definir y proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI son:

- Normalización y Culturización Contable
- Centralización de la Información
- Consolidación de la Información
- Planeación Integral
- Gestión Administrativa
- Gestión de Recursos Financieros
- Gestión Humana
- Gestión TICs

7.2 COMPETENCIA

Por medio del proceso de Gestión Humana se han determinado las habilidades y competencias requeridas para cada cargo y en función de los procesos establecidos, las cuales se registran en el documento *Manual Específico de Funciones y Competencias Laborales*. Además, el proceso de Gestión Administrativa selecciona personal especializado por prestación de servicios, quienes están en constante actualización en temas de seguridad de la información.

7.3 TOMA DE CONCIENCIA

Se realizan planes de capacitación y sensibilización en aspectos de seguridad de la información, haciendo énfasis en que los servidores públicos, colaboradores y las partes interesadas pertinentes tomen conciencia de la Política de Seguridad de la Información, las implicaciones de la violación de dicha política y sobre la manera en la cual pueden contribuir a la eficacia del SGSI.

7.4 COMUNICACIÓN

La CGN cuenta con el proceso estratégico de Comunicación Pública que apoya la divulgación de los aspectos relacionados con el SGSI. En adición a lo anterior, el GIT de Apoyo Informático ha definido el documento Excel *CGN-PLAN DE COMUNICACIONES*, donde se detalla por medio de una matriz de comunicaciones un plan con los temas de seguridad de la información para socializar, en el cual se incluye:

- ¿Qué comunicar?
- ¿Cuándo comunicar?
- ¿A quién comunicar?
- ¿Cómo comunicar?
- ¿Quién comunica?

7.5 INFORMACIÓN DOCUMENTADA

Los documentos que soportan el SGSI se encuentran para consulta en la intranet, siguiendo los lineamientos establecidos en el documento *PI-PRC04 Control de Documentos*, de conformidad con los requisitos de la Norma ISO 27001.

Por otra parte, el GIT de Apoyo Informático ha implementado un repositorio con los documentos que soportan la operación del GIT, incluida los de seguridad de la información.

8. OPERACIÓN

8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La planificación y control de la operación para la seguridad de la información de la CGN, se encuentra alineada con el alcance del SGSI para los procesos misionales y Gestión TICs; todos los productos y servicios se encuentran controlados por medio de la aplicación de políticas, manuales, procedimientos, instructivos y demás documentos que soportan los procesos de la entidad.

Así mismo, el procedimiento *GTI-PRC11 Administración de Activos TIC* tiene en cuenta los aspectos relacionados con el inventario y clasificación de activos, y asignación de su propietario, con el propósito de gestionar adecuadamente los riesgos que puedan afectar los activos de información. Además, por medio del

formato *GTI02-FOR04 Administración de Cambios a TI*, se identifican o registran los cambios sobre los activos para su respectivo control.

8.2 EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Con base a la metodología implementada para la valoración y tratamiento de los riesgos de la información, la CGN establece los lineamientos para llevar a cabo valoraciones de riesgos dos veces al año, o antes si se presentan cambios que ameriten realizar evaluaciones anticipadas.

De igual forma, la CGN conserva la información documentada de los resultados de las valoraciones de los riesgos de seguridad de información a través del documento *Mapa de Riesgos Institucional*.

Más información en:
https://www.contaduria.gov.co/web/intranet/sistema-de-gestion-de-calidad/-/document_library/vpkf13iCweJ8/view/2153685

8.3 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La metodología de administración de riesgos adoptada por la CGN considera que se implemente el plan de tratamiento de riesgos por medio del documento *Mapa de Riesgos Institucional*. Además, la CGN conserva la información documentada de los planes de tratamiento de los riesgos de seguridad de la información en el documento en mención. En concordancia con lo anterior, los controles para mitigar los riesgos de seguridad de la información se determinan siguiendo una selección de los controles enumerados en el Anexo-A de la Norma NTC/ISO 27001.

9. EVALUACIÓN DEL DESEMPEÑO

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La CGN genera mediciones, análisis y evaluación de la seguridad de la información y la eficacia del SGSI por medio de indicadores de gestión con base en el documento *PI-PRC22 Procedimiento Control Operacional Seguimiento y Medición*, dejando evidencia mediante el formato *PI19-FOR06 Hoja de Vida Indicador*.

El GIT de Apoyo Informático tiene implementados los indicadores de gestión de seguridad de la información con el documento Excel *TIC-GES-IND-2024-CuadroConsolidadoIndic* que contiene la ficha técnica de cada uno de ellos.

9.2 AUDITORÍA INTERNA

La CGN planifica y realiza auditorías internas para evaluar la conformidad del SGSI con los requisitos de la Norma ISO/IEC 27001, de acuerdo con lo indicado en el procedimiento *PI-PRC05 Auditorías Internas del Sistema Integrado de Gestión*.

9.3 REVISIÓN POR LA DIRECCIÓN

La Alta Dirección realiza revisiones planificadas del SGSI para asegurarse de su conveniencia, adecuación y eficacia continuas, de conformidad con lo indicado en el procedimiento *PI-PRC17 Revisión por la Dirección*.

10. MEJORA

10.1 NO CONFORMIDAD Y ACCIONES CORRECTIVAS

Cuando ocurra una no conformidad, la CGN actúa de acuerdo con lo establecido en el procedimiento *PI-PRC16 No Conformidades, Acción Correctiva, Preventiva y Planes de Mejoramiento*. Así mismo, las acciones correctivas adoptadas deben ser apropiadas a los efectos de las no conformidades encontradas. La CGN conserva información documentada como evidencia de las no conformidades y acciones correctivas mediante el formato *PI16-FOR01 Plan de Mejoramiento SIGI*.

10.2 MEJORA CONTINUA

La mejora se lleva a cabo a través de las acciones correctivas y de mejora, proporcionando así la mejora continua al SGSI. Además, constantemente se realizan actividades de capacitación con el fin de mantener la confidencialidad, integridad y disponibilidad de la información de la CGN y sus partes interesadas. Esto de conformidad con lo establecido en los siguientes procedimientos y formatos donde se pueden consultar los registros de las actividades planificadas para la implementación de la mejora continua:

- *PI-PRC16 No Conformidades, Acción Correctiva, Preventiva y Planes de Mejoramiento*
- *PI19-FOR02 Detalle de Actividades de Planes de Acción*

ANEXO-A

La CGN, mediante la implementación del SGSI, adopta el Anexo-A de la Norma ISO/IEC 27001, para determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos y contrastar estos frente a los controles del Anexo-A, y verificar que no sean omitidos controles necesarios. El documento *Herramienta de diagnóstico* incluye una declaración de aplicabilidad con los controles necesarios y la justificación de las inclusiones o exclusiones, si corresponde.