UNIDAD ADMINISTRATIVA ESPECIAL
CONTADURIA GENERAL DE LA NACIÓN

GRUPO INTERNO DE TRABAJO DE
APOYO INFORMÁTICO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2022

BOGOTA, NOVIEMBRE DE 2021

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO

Establecer desde el proceso Gestión Tics las medidas, actividades y controles de seguridad contempladas en el Anexo A de la norma NTC/IEC ISO 27001:2013 que ayudarán, mediante su implementación, a preservar la confidencialidad, integridad y disponibilidad de la información, así como la relación asociada a las políticas y procedimiento de Seguridad de la información que permitan asegurar la protección de esta.

2. ALCANCE

Aplica a todos los niveles de la U.A.E Contaduría general de la Nación - CGN, sus funcionarios, contratistas, proveedores y aquellas personas o terceros que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de información, ya sea interna o externamente independientemente de su ubicación, así mismo las actividades pertinentes que se consideren fundamentales para determinar la estrategia de implementación de los controles de seguridad requeridos para el funcionamiento adecuado del SGSI de la CGN.

3. 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 N° 193 del 19 de junio 2019.

4. ROLES Y RESPONSABILIDADES

Alta dirección:

- Aprobar anualmente o cuando se requiera la Política de Seguridad de la Información de la CGN

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

- 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 implementación
- Velar por 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.

Administrador del SGSI:

El rol del administrador del SGSI, es el responsable de:

- Realizar seguimiento al cumplimiento de los lineamientos y políticas del SGSI
- Revisar y aprobar políticas, planes, programas, procedimientos en materia de seguridad de la información para la aplicación de controles en el sistema
- Realizar revisiones al SGSI periódicamente y definir acciones a seguir
- Velar por el cumplimiento de las políticas, normas, procedimientos, y demás documentos relacionados con el SGSI

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

Coordinador de Grupo de Informática:

El GIT de apoyo informático y sus profesionales serán los responsables de los controles 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

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

- 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.

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

5. ACTIVIDADES

El Plan de implementación de Seguridad de la Información de la CGN comprende las siguientes actividades.

Id	Controles	Actividad 1	Actividad 2	Actividad 3	Responsable
1	Política general de seguridad de la información	Revisión anual del cumplimiento de la política general de seguridad de la información	Revisar y/o ajustar la política de seguridad de la información al menos cada año	Hacer seguimiento a las evidencias de actualización y revisión del cumplimiento de la política de seguridad	Alta Dirección Planeación Integral
2	Manual de seguridad de la información	Revisión del Manual de Seguridad de la Información	Actualización del Manual de Seguridad de la Información	Realizar seguimiento del Manual de Seguridad de la Información	Gestión Tics
3	Procedimiento de seguridad de la información	Realizar seguimiento y control del	Revisar y/o actualizar los documentos	Solicitar a Planeación la actualización de	Gestión Tics

		procedimiento, formatos, instructivos, políticas, etc.	asociados al procedimiento GTI-PRC010 Seguridad de la información	los documentos y publicación de estos.	Planeación Integral
4	Gestión de activos de Información	Levantamiento y/o actualización de los Activos de Información	** Identificar nuevos activos de información en cada área ** Validar la actualización de los activos de información en el formato actualizado comparado con la vigencia anterior	** Verificación y aprobación de los activos de información para su publicación en Intranet ** Publicar los activos de información consolidado	Planeación Integral Todos los procesos del alcance del SGSI
5	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	** 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.	Gestión Tics

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

6	Indicadores de seguridad de la información	Formular, Implementar y actualizar los indicadores del SGSI	**Realizar seguimientos a las acciones correctivas planteadas para los indicadores que no cumplen las metas **Realizar seguimiento al cumplimiento de las metas de los indicadores del SGSI	Hacer seguimiento a las evidencias de ejecución de acciones correctivas o de mejora	Planeación integral Gestión Tics
7	Gestión de riesgos (Identificación, Análisis y Evaluación de Riesgos)	Realizar seguimiento trimestral de los Planes de Tratamiento de Riesgos	Realizar valoración trimestral del riesgo residual	Realizar seguimiento a la Documentación y evidencia de la ejecución del Plan de Tratamiento de Riesgos	Planeación Integral Gestión Tics Líderes de los procesos misionales de la CGN
8	Plan de contingencia y continuidad de negocio de TI	** Actualización del documento ** Identificación y/o valoración de Riesgos de interrupción de la operación de la entidad	** Realizar seguimiento y revisión de la ejecución de las pruebas del plan ** 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	Gestión Tics
9	Plan de comunicación,	** Elaborar y ejecutar el Plan de comunicación	Realizar evaluación de conocimientos	Hacer seguimiento a las evidencias	Planeación Integral

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

	socialización y sensibilización	en temas relacionados con seguridad de la información ** Realizar mínimo 2 jornadas de sensibilización en seguridad de la información en las jornadas de inducción y reinducción durante el año	de seguridad posterior a las capacitaciones (Encuestas)	de socialización del SGSI	*** Líderes de los procesos de la CGN (Nota: Los lideres podrán realizar socializaciones internas de seguridad de la información cuando sea pertinente mas no es obligatorio)
10	Auditoria (Internas – Externas)	Realizar auditorías internas y externas de la norma ISO 27001:2013	Realizar seguimiento al cierre de las no conformidades producto de las auditorías internas y externas al SGSI.	Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso	Planeación Integral Todos los procesos del alcance del SGSI
11	Gestión de incidentes de seguridad	Gestionar los incidentes de Seguridad de la Información identificados	**Realizar el seguimiento a la gestión de incidentes de seguridad de la información incluyendo cierre **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.	Gestión Tics

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

12	Declaración de aplicabilidad - AnexoA	Revisión de los controles de la norma ISO 27001:2013	Actualizar declaración aplicando acciones y controles para la implementación del control	Seguimiento a la aplicación de los controles	Gestión Tics

6. 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

Elaboró: Ing. Diego Camelo Ávila – Ing. Lorena Sofía Valderrama M.
Revisó: Ing. Martha Patricia Zornoza G.
Aprobó: Ing. Gustavo Adolfo González Escobar.

Dirección: Calle 26 # 69 -76 | Edificio Elemento
Torre 1 (Aire) - Pisos 3 y 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00