UNIDAD ADMINISTRATIVA ESPECIAL
CONTADURÍA GENERAL DE LA NACIÓN - CGN

Manual de Seguridad de la Información y Digital

Diciembre, 2023

CONTROL DE CAMBIOS

VERSIÓN	SECCIÓN	TIPO	FECHA (DD/MM/AAAA)	AUTOR	OBSERVACIONES
6.0	Todas	Actualización	13/10/2022	GIT de Apoyo Informático	Actualización
7.0	Todas	Actualización	29/11/2023	GIT de Apoyo Informático	- Corrección en la numeración de la tabla de contenido - Reorganización del contenido - Mejora en la redacción del documento - Inclusión de Política de Clasificación de Información - Inclusión de Política de red interna de la CGN - Eliminación de textos con políticas externas, incluyendo solo las referencias

Contenido

1. Descripción

La Contaduría General de la Nacional (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 misionales. Con prioridad en garantizar la confidencialidad, disponibilidad e integridad de la información a través de prácticas sólidas de seguridad digital.

En línea con las directrices del Gobierno Nacional sobre seguridad y privacidad de la información, la CGN se dedica a proteger los datos personales, el habeas data, el buen nombre de la Contaduría General de la Nación (CGN) y de terceros con los que la Entidad tenga vínculos. Para lograrlo, aplicamos metodologías de valoración y tratamiento de riesgos que se ajustan a nuestras necesidades organizacionales.

El presente Manual de Seguridad de la Información y Digital refleja la postura de la CGN en cuanto a la protección de los activos de información, la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y el respaldo, desarrollo y publicación de nuestras políticas, procedimientos e instructivos.

En nuestra búsqueda por cumplir nuestra misión, visión y objetivos estratégicos, así como nuestros valores institucionales, hemos establecido la función de Seguridad de la Información en la Entidad, con los siguientes objetivos:

• Operar y mantener el sistema de gestión de seguridad de la información, que incluye salvaguardar nuestra infraestructura tecnológica y digital.
• Establecer políticas, procedimientos e instructivos claros y precisos en materia de seguridad de la información y digital.
• Adoptar y aplicar los principios y mejores prácticas de seguridad de la información y digital.
• Gestionar y mitigar los riesgos de seguridad de la información y digital.
• Mantener la confianza de nuestros servidores públicos y demás usuarios externos en cuanto a la seguridad de sus datos y la información que manejan.
• Promover una cultura de conciencia en torno a la importancia de proteger la información y los datos que se encuentran y se procesan.
• Identificar y abordar los riesgos, para prevenir, mitigar o actuar en caso de incidentes de seguridad y digital que puedan afectar a los servidores públicos, terceros y demás partes interesadas de la CGN.
• Contribuir con continuidad del negocio frente a incidentes de seguridad, digital y privacidad de la información, mediante la implementación de medidas de seguridad efectivas.
• Fomentar y respaldar la innovación tecnológica, teniendo en cuenta los

aspectos de seguridad digital.

Con esta orientación en seguridad de la información y digital, la CGN está comprometida a proteger nuestra información y sistemas en un entorno cada vez más digitalizado y en constante evolución.

2. Referencia normativa

Ley 603 de 2000: Esta Ley se refiere a la protección de los derechos de autor en Colombia. Recuerde:el software es un activo, además está protegido por el Derecho de Autor y obliga a las empresas a declarar si los problemas de software son o no legales.

Ley Estatutaria 1266 del 31 de diciembre de 2008: Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales.

Ley 1273 del 5 de enero de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevobien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Ver esta Ley.

Artículo 230 de la Ley 1450 de 2011 estableció que todas las Entidades deben adelantar acciones señaladas por el Gobierno Nacional, concernientes a implementar las estrategias de Gobierno en Líneaque se definen por el Ministerio de Tecnologías de la Información y las comunicaciones.

Decreto No. 2693 de 2012, respalda el Manual de Gobierno en Línea y trae inmerso el manual de seguridad, creando los lineamientos, plazos y términos para el mejoramiento de las Tecnologías de la Información y las Comunicaciones.

Ley Estatutaria 1581 De 2012, Protección de Datos Personales, sancionada siguiendo los lineamientosestablecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Decreto 1377 De 2013: Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581de 2012. Añade dos nuevos capítulos al Código Penal Colombiano:

Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;

Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver en elprimer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas coneste tema.

Ley 1712 de 2014: Ley de transparencia y acceso a la información pública;

Decreto No. 2573 de 2014, establece como lineamiento la Seguridad y privacidad de la Información y comprende acciones transversales además de componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instruccionessobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que seencuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Decreto 415 de 2016: Por el cual se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimientoinstitucional en materia de tecnologías de la información y las comunicaciones";

Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de GobiernoDigital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, DecretoÚnico Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

Decreto 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción

Ley 1952 de 2019: por medio de la cual se expide los PRINCIPIOS Y NORMAS RECTORAS DE LA LEY DISCIPLINARIA y se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.

Resolución 193 de 19 de junio de 2019, por el cual se crea el Sistema de Gestión y Desempeño de laUnidad Administrativa Especial (UAE) Contaduría General de la Nación (CGN) y se dictan otras disposiciones.
CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad Digital

Resolución 500 de 2021, Por la cual se establecen los lineamientos y estándares para la estrategia deseguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Decreto 338 de 2022, "Por el cual se adiciona el Titulo 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer

la gobernanza de la seguridad digital, secrea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

Resolución 746 de 2022, Por el cual se fortalece el Modelo de Seguridad y Privacidad de la Informacióny se definen los lineamientos adicionales a los establecidos en la Resolución 500 de 2021.
Directiva Presidencial No 02 de 2022, Reiteración de la Política pública en materia de seguridad digital.

Resolución 767 de 2022, Por el cual se fortalece el Modelo imparten lineamientos generales de la Política de Gobierno Digital y otras disposiciones y en particular lo referente a las como Habilitador transversal de la Seguridad y Privacidad de la Información.

Resolución 163 de 2022 - CGN. Por la cual se adopta la modalidad de Teletrabajo en la Unidad Administrativa Especial (UAE) Contaduría General de la Nación (CGN).

Circular No 004 de 2022 - CGN, la cual establece las pautas de Seguridad de la Información a aplicaren la Unidad Administrativa Especial (UAE) Contaduría General de la Nación (CGN) – Teletrabajo.

Norma Técnica Colombiana NTC-ISO-IEC 27001:2013. Norma técnica de sistemas de gestión de seguridad de la información.

3. Definiciones

Acción correctiva: remediación de los requisitos o acciones que dieron origen al establecimiento de una NO Conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: disposición de operaciones que buscan de forma preliminar, que no se presente ensu ejecución, desarrollo e implementación una NO Conformidad.

Aceptación del Riesgos: decisión relativa a la tolerancia o no del riesgo asociado con una exposición determinada de las consecuencias que puede acarrear el mismo.

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.

Activos TIC: recursos de sistema de información o relacionados con éste, necesarios para que la Entidad funcione correctamente y alcance los objetivos estratégicos propuestos por la Alta Dirección. Sepueden estructurar en las

siguientes categorías: software, hardware, servicios, datos, personas, proveedores, instalaciones físicas, comunicaciones, equipamiento, etc.

Acuerdo de Confidencialidad: contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

Amenaza: en el contexto de seguridad de la información, es cualquier circunstancia, evento o acción que tiene el potencial de causar daño, degradar la seguridad o comprometer los activos de la Entidad. Estas amenazas pueden surgir tanto de fuentes internas como externas y pueden ser intencionadas o accidentales.

Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Batch (Instrucciones en lote): archivo magnético que tiene almacenada una secuencia de comandos. Al ejecutarse, reemplazala operación de digitar los comandos de secuencia cada vez que se requiere efectuar una operación. Se utiliza para almacenar operaciones repetitivas.

CGN: sigla – Contaduría General de la Nación

Ciberamenaza: se refiere a aquellas actividades 'malignas' que tienen lugar en un entorno digital, para acceder o dañar un sistema de computadoras o redes.

Ciberseguridad: se refiere a las actividades y medidas necesarias para proteger los activos de información, como la información procesada, almacenada y transportada por los sistemas de información interconectados. Su objetivo principal es mitigar las amenazas que ponen en riesgo dicha información, así como proteger las redes, los sistemas de información, los usuarios involucrados y otros afectados por las ciberamenazas.

Ciberespacio: es el espacio (no físico) o entorno digital desarrollado por computadoras.

Ciberdefensa: conjunto de lineamientos, procedimientos o estrategias preventivas o reactivas desarrolladas e implementadas para gestionar las transacciones del entorno digital.

ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT.

Confiabilidad: propiedad que determina que la información no se haga

disponible ni sea revelada a individuos, Entidades o procesos no autorizados.

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.

Control de acceso: el proceso que limita y controla el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido por el sistema (mandatory access control – MAC), o definido porel usuario propietario del objeto (discretionary access control – DAC).

CSIRT Gobierno: (CSIRT, del inglés Computer Security Incident Response Team, Equipo de Respuestaante Incidencias de Seguridad Informáticas). Es un equipo de respuesta ante emergencias informáticaso un centro de respuesta a incidentes de seguridad en tecnologías de la información del gobierno.

CSIRT-PONAL: (CSIRT, del inglés Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas). Equipo de Respuesta a Incidentes de Seguridad Informáticade la Policía Nacional CSIRT-PONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.

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.

Encriptación (Cifrado, codificación): la encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.
Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada queno debería ser accesible a terceros. Pueden ser

contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

Evento: un evento en la seguridad de la información es un cambio en las operaciones diarias de una red o servicio de tecnología de la información que indica que una política de seguridad puede haber sidoviolada o que un control de seguridad puede haber fallado.

Firewall (Muro de fuego): dispositivo tecnológico que tiene como función proteger la red interna de una compañía de accesos no autorizados del exterior vía Internet.

Gestión de Riesgos: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

GIT: sigla - Grupo Interno de Trabajo institución.

Impacto: el costo para la entidad de un incidente de la escala que sea, que puede o no ser medido entérminos estrictamente financieros p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de Seguridad: 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.

Internet: es un sistema mundial de redes de computadoras interconectadas para compartir información.

Medio Removible y extraíbles: se define como medio removible todo dispositivo de almacenamiento de información que sea extraíble de su fuente de información o todo lo que permita almacenar y transportar información.

Módem: dispositivo de comunicación que permite establecer una conexión a través de la líneatelefónica.

Oficial de Seguridad de la Información: persona o área delegada por la alta dirección cuyas funciones principales son asesorar en materia de seguridad de la información a la CGN y supervisar el cumplimiento de la presente Política.

Password: palabra en inglés que significa contraseña, clave o llave. Es la forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso o servicio tecnológico.

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. (Tomado de PLAN DE TRATAMIETO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MinTIC)

Rol: es un conjunto de permisos que puede asignarse a un usuario que se registra en un sistema.

RDP: la sigla RDP significa *Remote Desktop Protocol*, en español, Protocolo de Escritorio Remoto. El protocolo RDP, entonces, permite que el escritorio de un equipo informático sea controlado a distancia por un usuario remoto.

Red Privada Virtual – VPN: metodología de conexión vía Internet que permite a los usuarios conectarse a la red corporativa utilizando conexiones públicas, a través de canales seguros de comunicación.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Script: archivo que contiene una secuencia de comandos que se utiliza para comunicarse en forma automática entre dos aplicaciones.

Seguridad digital: la protección y conservación de la información y datos en línea para que no sean robados, dañados o comprometidos.

Seguridad Informática: es el conjunto de tecnologías, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, daño o acceso no autorizado.

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

Sistema de Información: se refiere a un conjunto de recursos organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de

información según determinados procedimientos, tanto automatizados como manuales.

Teletrabajo: es el término bajo el cual se conoce el esquema acordado formalmente entre un empleado y su empleador para trabajar en un lugar diferente a la oficina. El aprovechamiento de las ventajas de las Tecnologías de información y comunicación permite lograr las actividades en forma no presencial, trayendo consigo la ventaja de evitar pérdidas de tiempo en desplazamiento y poder trabajardesde la comodidad de su lugar de vivienda.

Token: (vale digital) es una herramienta digital o física que genera una clave irremplazable de forma aleatoria y temporal. El *token* se utiliza como complemento o en lugar de una contraseña.

Tercero(s): Cualquier persona natural o jurídica en calidad de proveedor, outsourcing o consultor.

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

4. Cumplimiento y Principios

El cumplimiento de las políticas de seguridad deberá ser acogido por todos los servidores públicos, contratistas, terceros y personal externo que tenga acceso o relación con los recursos o los activos de información de la Entidad. Si un individuo u organización viola las disposiciones establecidas en las Políticas de seguridad de información y digital, por negligencia o intencionalmente, la Contaduría General de la Nación tomará las medidas correspondientes de acuerdo con lo establecido en los PRINCIPIOS Y NORMAS RECTORAS DE LA LEY DISCIPLINARIA (Ley 1952 de 2019).

Los principios de cumplimiento que se deben seguir para cubrir el alcance y aplicabilidad del SGSI son:

a. Operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y los requerimientos regulatorios.

b. Las responsabilidades frente a la seguridad de la información son definidas, compartidas, publicadas y aceptadas por cada uno de sus servidores públicos, terceros, aprendices, practicantes, proveedores y demás partes interesadas.

c. Proteger la información generada, procesada, transmitida o

resguardada por los procesos de la entidad, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

d. Proteger la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta. Para ello es fundamental la aplicación de controles, de acuerdo con la clasificación de la información de su propiedad o en custodia.

e. Proteger la información de las vulnerabilidades y amenazas del entorno interno y externo.

f. Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.

g. Controlar la operación de los procesos de la Entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.

h. Implementar control de acceso a la información, sistemas y recursos de red.

i. Garantizar que la seguridad y privacidad de la información sea parte integral del ciclo de vida delos sistemas de información.

j. Garantizar que a través de una adecuada gestión de los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

k. Garantizar la disponibilidad tecnológica que soporta los procesos de la Entidad y la continuidadde su operación basada en el impacto que pueden generar los eventos.

l. Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

5. Propósito

El Manual de Seguridad de la Información y Digital de la Contaduría General de la Nación (CGN) establece políticas y objetivos para proteger los activos de información en los ámbitos físico y digital. Su objetivo principal es reducir el riesgo de divulgación, modificación o uso indebido de los activos de información y operaciones críticas, incluyendo la seguridad digital. Este enfoque se orienta

en mejorar la administración de la seguridad de los activos, detectar amenazas y fomentar una cultura de control, conciencia y responsabilidad en la CGN. El compromiso se extiende a la protección de datos en el entorno físico y digital, asegurando la integridad, confidencialidad y disponibilidad de la información. La CGN se compromete a implementar y mantener políticas y prácticas de seguridad de la información y digital efectivas, monitorear los riesgos y contribuir a la seguridad y continuidad de sus operaciones en el mundo digital.

6. Alcance

El presente documento establece los lineamientos para garantizar la seguridad de la información digital mediante la protección de la confidencialidad, integridad y disponibilidad de los activos de información en toda la Entidad. Estos lineamientos se aplican tanto a los funcionarios de la Contaduría General de la Nación (CGN) como a los contratistas, terceros y partes interesadas que mantengan una relación directa con la entidad.

Teniendo en cuenta el siguiente **alcance del Sistema de Gestión de Seguridad de la Información de la CGN**:

"La Contaduría General de la Nación define su alcance para el Sistema de Gestión de Seguridad de la Información y Digital en las siguientes actividades: 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, de acuerdo con la Declaración de Aplicabilidad vigente. Cuya sede está ubicada en la calle 26 No. 69 - 76. Edificio Elemento Torre 1 (Aire) 15 de la Ciudad de Bogotá."

7. Generalidades

Las políticas de seguridad de la información, descritas en este Manual, son aplicables a todos los activos de información durante su ciclo de vida, desde su creación hasta su eliminación. Estas directrices están diseñadas para asegurar el uso apropiado de los servicios de TI.

El objetivo primordial de estas políticas es proporcionar lineamientos claros para el uso seguro y adecuado de los recursos tecnológicos y digitales de la Contaduría General de la Nación (CGN). Se busca minimizar los riesgos asociados con la posible pérdida de activos de información sensibles para la organización.

Esto conlleva la adopción de medidas de seguridad apropiadas durante el almacenamiento, transmisión, distribución y eliminación de los activos de información. Además, se promoverá la concientización y capacitación en seguridad digital para fortalecer la postura de seguridad de la institución y

prevenir amenazas y ataques cibernéticos.

Es responsabilidad de todos los involucrados en la organización conocer y cumplir con estas políticas de seguridad de la información y usar los recursos tecnológicos de manera responsable y segura. La implementación efectiva de estas políticas contribuirá a salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información, protegiendo la reputación e intereses de la institución en un entorno digital cada vez más complejo y cambiante.

Todo evento o incidente de seguridad deberá ser reportado al correo seguridadinformatica@contaduría.gov.co

8. Política del SGSI - Sistema de Gestión de Seguridad de la Información de la CGN

La Contaduría General de la Nación como autoridad rectora responsable de regular la contabilidad general de la nación, 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 cual, la Contaduría establece estrategias y controles en el marco de un Sistema de Gestión de Seguridad de la Información (SGSI), que forma parte del Sistema Integrado de Gestión de la Entidad, asegurando la disposición de recursos requeridos y un enfoque basado en la gestión de los objetivos de seguridad de la información, gestión de riesgos de seguridad de la información, la gestión de incidentes de seguridad de la información y la mejora continua.

La CGN, se compromete a garantizar, verificar y cumplir todos los requerimientos operativos, normativos, legales y de otra índole aplicables a la seguridad de la información.

9. Objetivos del Sistema de Gestión de Seguridad de la Información.

a. 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 27001:2013.
b. Asegurar la protección de los activos informáticos de apoyo en los procesos misionales.
c. Identificar y dar cumplimiento a los requisitos legales y regulatorios, así como a las obligaciones contractuales de la Contaduría General de la Nación.

d. 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.
e. 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, además en el reporte de eventos e incidentes de seguridad.

10. Revisión de la política y el manual de seguridad de la información y digital

La política general y el manual de políticas de seguridad de la información y digital es revisado y actualizado (en caso de ser necesario) al menos una vez al año o cuando haya cambios relevantes en el contexto estratégico de la Contaduría General de la Nación, con el fin de asegurar que sigan siendo adecuados a la estrategia y necesidades de la Entidad. Estos documentos son revisados por la Alta Dirección con el apoyo del Oficial de Seguridad de la Información o quien haga sus veces y aprobados por el Comité Institucional de Gestión y Desempeño.
Las políticas y el manual de políticas de seguridad de la información y digital deberán ser aprobadas por el Comité Institucional de Gestión y Desempeño y estar acorde a los lineamientos de la CGN.

11. Roles y Responsabilidades

a. *RESPONSABLE DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*

El responsable de la seguridad y privacidad de la información tendrá las siguientes responsabilidades:

- Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información. realizando la implementación y seguimiento de estos.
- Coordinar la gestión de riesgos según la periodicidad establecida, incluyendo la actualización de amenazas, vulnerabilidades y riesgos en los activos de información de la organización.
- Dictar lineamientos para controlar el acceso a los sistemas de información y la modificación de los privilegios.
- Hacer seguimiento a las no conformidades y al estado de las acciones correctivas, relacionadas con la seguridad de la información.
- Asegurar que se establecen, mantienen e implementan los procesos necesarios para el desarrollo del Sistema de gestión de seguridad de la información, SGSI.

- Presentar los informes del SGSI, incidentes de seguridad de la información, así como las lecciones aprendidas.
- Apoyar las reuniones del Comité Institucional de Gestión y Desempeño para tratar los asuntos relacionados con la seguridad de la Información que se requieran o cuando se presente la materialización de un incidente de seguridad de la información.
- Garantizar la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Informar a la Alta Dirección sobre el desempeño del Sistema de Gestión de Seguridad de la Información.
- Mantener contacto con grupos especiales en temas de seguridad de la información, con el fin de estar actualizado acerca de nuevas amenazas.
- Coordinar las actividades correspondientes a la gestión de Incidentes de Seguridad de la información.
- Desarrollar, mantener y comunicar las políticas, estándares y guías de seguridad de la información.
- Identificar y reportar riesgos, eventos o incidentes de seguridad a través de los canales definidos.
- Realizar el proceso de gestión de incidentes de seguridad que se presenten en la organización.
- Dar soporte y asesoría a los líderes de proceso en el análisis de riesgos de seguridad de la información, así como consolidar los planes para su tratamiento.
- Elaborar las campañas de sensibilización y socialización del SGSI.
- Coordinar junto con el responsable de infraestructura el fortalecimiento servidores, enrutadores.
- Configurar y afinar las herramientas de seguridad instaladas.

b. RESPONSABLE DE INFRAESTRUCTURA

El responsable de infraestructura en aras de asegurar el correcto uso y administración de los recursos tecnológicos de la Entidad y para coadyuvar a la seguridad de la información en la CGN tendrán las siguientes responsabilidades dentro del SGSI:

- Identificar y actualizar en conjunto con el responsable de la seguridad y privacidad de la información el inventario de activos de información y apoyar al líder del proceso en la valoración y determinaran la criticidad de los activos identificados.
- Planear y ejecutar el plan de mantenimiento de la infraestructura tecnológica de la organización.
- Implementar las mejoraras identificadas por el SGSI que estén relacionadas con hardware, software, canales de comunicaciones o infraestructura de TI en general.

- Identificar y reportar riesgos, eventos o incidentes de seguridad a través de los canales definidos.
- Gestionar recursos para la mejora continua del SGSI.

c. LÍDERES DEL PROCESO

Los líderes de procesos son los responsables y propietarios de los activos de información para todos los aspectos de seguridad de la información y deben cumplir las siguientes responsabilidades dentro del SGSI:

- Identificar e incluir en el inventario de activos de información los activos identificados, así como los riesgos asociados.
- Revisar los informes de auditorías efectuadas al SGSI y velar porque se ejecuten las acciones correctivas identificadas, así como las oportunidades de mejora y recomendaciones dejadas por los auditores.
- Efectuar el análisis de riesgos de seguridad de la información en sus procesos y activos de información y coordinar el plan tratamiento de los riesgos identificados con el líder de seguridad de la información.
- Identificar oportunidades de mejora en seguridad de la información en sus procesos.
- Realizar acompañamiento al responsable de la seguridad y privacidad de la información y al responsable de infraestructura en la identificación y clasificación de los activos de información.

12. Separación de deberes

a. Todo aquel que tenga acceso a la información de la CGN, debe tener claramente definidas sus funciones, con el fin de reducir el uso no autorizado, indebido o accidental de los activosde información.

b. Todos los sistemas de información de la CGN deben implementar reglas de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga los privilegios y quien lo utiliza.

13. Contacto con Autoridades y Grupos de interés

a. La CGN, mantiene contacto con las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes. Adicionalmente, el proceso de Gestión TICs cuenta con un directorio actualizado de autoridades y grupos de interés.

b. El proceso de Gestión TICs en conjunto con el Oficial de Seguridad o quien haga sus veces mantendrán contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información; de acuerdo al tipo, criticidad e impacto del incidente, el Líder de Seguridad de la Información definirá con cuales de las siguientes organizaciones de control y monitoreo de infraestructuras cibernéticas públicas o privadas, se compartirá o escalará la incidencia para su tratamiento:
   - ColCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
   - CSIRT PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional.
   - CSIRT GOB – Grupo de respuesta a incidentes del Ministerio de Tecnologías de la Información y Comunicaciones

Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información y recibir advertencias de actualizaciones, ataques, y vulnerabilidades del software y firmware utilizado en la Contaduría General de la Nación.

La administración del edificio cuenta con los números de contacto actualizados de las autoridades y deberá estar en contacto con el Oficial de Seguridad o quien haga sus veces para atender los incidentes que se presenten y requieran de estos contactos. Manual de Seguridad Física, código SF-MA-01.

14. Políticas de Seguridad de la Información y Digital

A continuación, se describen las políticas de seguridad de la información y digital

14.1. Política de Clasificación de Información

La Contaduría General de la Nación ha adoptado un sistema de clasificación de la información que la categoriza en tres grupos de acuerdo con su grado de confidencialidad. Toda la información bajo control de la Contaduría General de la Nación generada interna o externamente se encuentra en una de estas categorías:

Pública: Información que puede ser divulgada al público en general sin restricciones.

Pública Clasificada: Información pública que requiere ciertos niveles de control o autorización adicional debido a su naturaleza sensible o estratégica.

Pública Reservada: Información pública altamente confidencial que requiere niveles máximos de protección y autorización para su acceso y divulgación.

Todos los servidores públicos deben familiarizarse con las definiciones de estas categorías y cumplir con las medidas de protección establecidas para ellas.

14.2. Política Seguridad de la Información en la Gestión de Proyectos

La seguridad de la información se debe integrar a la gestión de proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de los proyectos. Lo anterior aplica a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los coordinadores y líderes de procesos asegurar que se sigan las siguientes directrices:

a. Incluir objetivos de seguridad de la información en los objetivos del proyecto.

b. Realizar valoración de los riesgos de seguridad de la información en la fase de estudiosprevios del proyecto, para identificar los controles necesarios.

c. Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todaslas fases del proyecto.

14.3. Política de Dispositivos Móviles

Los dispositivos móviles que son propiedad de la CGN, utilizados dentro o fuera de la Contaduría General de la Nación y en funciones propias de la Entidad, deben ser exclusivamente utilizados para brindar apoyo a las actividades de la Entidad y deben ser sujetos a un grado equivalente de protección al de los equipos que se encuentran dentro de las instalaciones de la Contaduría General de la Nación. Por lo tanto, se deben aplicar las siguientes pautas:

Dispositivos Móviles

a. Para la utilización de los dispositivos móviles se deben cumplir con las políticas: GTI10-POL01 - POLÍTICA DE ACCESO A LA RED PRIVADA VIRTUAL DE LA CGN y GTI10-POL03 Política para el Uso de la Red Inalámbrica Pública en la CGN.
b. Durante los viajes, los equipos (y medios) no se deben dejar desatendidos en lugares públicos. Las computadoras portátiles se deben llevar como equipaje de mano.
c. Los portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Seles deben proporcionar una forma apropiada de protección al acceso (ej. Contraseñas de encendido, encriptación, etc.) con el fin de prevenir acceso no autorizado.
d. Las instrucciones del fabricante concernientes a la protección del

equipo se deben seguir en todo momento (ej.: para protegerse contra la exposición de campos electromagnéticos muy fuertes).

e. Los equipos de cómputo de la CGN, así como la información almacenada en los mismos, son propiedad de la Contaduría General de la Nación, y pueden ser inspeccionados, o utilizados de cualquier manera y en cualquier momento en que la Entidad lo considere. Estos deben ser devueltos a la CGN en el momento en que el usuario termine la relación laboral con la Entidad.
f. Un equipo portátil, teléfono inteligente o cualquier otro sistema de cómputo usado para actividades de la CGN que contenga información sensible, no se deberá prestar a nadie y será responsabilidad exclusiva del funcionario que lo tenga asignado.
g. Las estaciones de trabajo y equipos portátiles que son propiedad de la CGN cuentan consoftware licenciado y protección contra código malicioso.
h. El contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto delcontrato deberá:

- Usar software legal instalado en el equipo.
- Contar con software antivirus licenciado.
- La CGN se reserva el derecho de monitorear y revisar cuando se requiera, el software instalado en los equipos de cómputo y servidores conectados a la red de la Entidad.

14.4. Política de Teletrabajo y Trabajo Remoto

La CGN establece los lineamientos de Teletrabajo en la Resolución 224 de 2022, por la cual se adopta la modalidad de Teletrabajo en la Unidad Administrativa Especial Contaduría General de la Nación CGN, donde se establecen los mecanismos de adopción, modalidad y obligaciones generales de los servidores públicos o colaboradores.

En concordancia con lo anterior, la CGN establece los mecanismos de control para preservar los niveles de seguridad de los activos de información requeridos para el desarrollo de las actividades de teletrabajo o trabajo remoto por parte de los servidores públicos o colaboradores.

La CGN define los canales de comunicación tales como el establecimiento de VPN`s y métodos de autenticación apropiados para controlar el acceso remoto de los usuarios a la información o sistemas de información de La CGN o de los clientes.

Los colaboradores en modo teletrabajo, trabajo remoto o conectados vía VPN se habilitan para que ingresen a los sistemas de información locales y se llevará registro de su conexión, y los permisos de navegación a internet estarán limitados a su conexión propia teniendo en cuenta las buenas prácticas para el aseguramiento de la información.

Los servidores públicos o colaboradores en la modalidad de teletrabajo o trabajo

remoto deben cumplir con los siguientes aspectos:

a. Hacer uso adecuado y exclusivo de los recursos tecnológicos informáticos aprobados para el cumplimiento de las funciones o actividades asignadas.
b. Asegurarse de mantener la debida integridad, confidencialidad, disponibilidad y privacidad de la información.
c. Abstenerse de instalar software o programas ejecutables en los equipos asignados, sin previa autorización del GIT de Apoyo Informático, quien se reserva el derecho de verificar la necesidad y las implicaciones de seguridad de su instalación.
d. Está prohibido el envío de archivos con información de la CGN, por medios no oficiales, tales como dropbox, WeTransfer, correos de dominio gratuito, etc.
e. La sesión establecida con la CGN no debe ser utilizada por una persona diferente al servidor público o colaborador autorizado.
f. No deben establecerse conexiones desde un sitio de acceso público como un café internet, aeropuerto y restaurante, entre otros.
g. Establecer conectividad con el equipo de cómputo prestado para teletrabajo o trabajo remoto
h. Reportar cualquier evento anormal aplicando la Gestión de Incidentes de seguridad.

14.5. Política Capacitación y Entrenamiento en Seguridad de la Información

La Contaduría General de la Nación en cabeza del Oficial de Seguridad o quien haga sus veces, realizará actividades de inducción, reinducción y capacitaciones (Internas – Externas) a funcionarios y contratistas con el fin de asegurar que se tengan en uso las políticas de seguridad de la información de la CGN, las cuales se enmarcan en la apropiación de los controles propuestos en el Anexo A de la norma NTC ISO/IEC 27001:2013; cuidado de los activos de información, adopción y medición de las políticas; sensibilizando sobre el adecuado uso y responsabilidades sobre los activos asignados, y sensibilizando sobre los diferentes temas relacionados con la gestión de activos y gestión de riesgos digitales. Esto se realiza desacuerdo a la Estrategia de Uso y Apropiación de TI.

14.6. Política Procesos Disciplinarios

Los procesos disciplinarios en la Contaduría General de la Nación se llevan a cabo de acuerdo con la Ley 1952 de 2019 (PRINCIPIOS Y NORMAS RECTORAS DE LA LEY DISCIPLINARIA), por parte de secretaria general.

14.7. Política de Intercambio de Información

a. La Contaduría General de la Nación firma un compromiso de confidencialidad con los servidores públicos y con terceros (contratistas y proveedores) que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información pública clasificada o pública reservada de la Entidad. En este compromiso quedan especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firman antes de permitir el acceso o uso de dicha información.
b. El procedimiento de gestión de activos de información contiene las directrices a tener en cuenta a la hora de intercambiar información catalogada como pública clasificada o pública reservada.
c. El intercambio de información con organismos de control y autoridades de supervisión se rige por las directrices de dichos entes externos para el intercambio de información, tales como, uso de aplicaciones específicas, tokens y firmas digitales.

14.8. Política de Gestión de Activos

La Política de Gestión de Activos establece principios y procedimientos para administrar eficientemente los recursos de la CGN, optimizando su rendimiento y maximizando su valor. Se enfoca en la adquisición, uso, mantenimiento y disposición de activos para alinearlos con los objetivos organizacionales, fomentando la transparencia, el cumplimiento normativo y la mejora continua en la toma de decisiones relacionadas con los activos de la empresa.

16.8.1. Inventario de activos:

El Oficial de Seguridad de la Información o quien haga sus veces vela porque los líderes de procesos anualmente identifiquen y documenten el inventario de activos de información, siguiendo las indicaciones del procedimiento PI-PRC28 - Gestión de activos.

16.8.2. Asignación de activos:

La asignación de equipo de cómputo se realiza de acuerdo con las obligaciones del servidor público o contratista y requerimientos solicitados por el líder del proceso.

16.8.3. Uso aceptable de los activos:

a. La información (física y digital), y los sistemas de información, servicios, y equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la CGN, son activos de la Entidad y se proporcionan a los empleados, contratistas y

terceros autorizados, para cumplir con los propósitos del negocio.

b. La información será etiquetada y deberá dar un manejo adecuado según su clasificación, siguiendo las directrices del procedimiento de Gestión de activos la Información (PI-PRC28) y el instructivo de Gestión de Activos de Información (PI28-INS01) y formato (PI28-FOR01).

c. Los equipos informáticos que son adquiridos por la Entidad deberán etiquetarse en el área de almacén antes de que sean asignados.

d. En caso de que el colaborador deba hacer uso de equipos ajenos a la CGN, estos deberán cumplir con la legalidad del software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red de la CGN una vez esté autorizado por el líder del proceso.

14.9. Política para el uso de medios removibles, borrado seguro y disposición de medios

Las especificaciones están definidas en la Política para el Uso de Medios Removibles, Borrado Seguro y Disposición de Medios GTI010-POL04.

14.10. Política de Administración de Usuarios y Contraseñas

La Política de Administración de Usuarios y contraseñas se realiza de acuerdo con las especificaciones definidas en la Política de Administración de Usuarios y Contraseñas GTI02-POL01.

a. El registro e inhabilitación de usuarios; el suministro de acceso a usuarios; la gestión de derechos de acceso privilegiado; la gestión de información de autenticación secreta; y la revisión, retiro o ajuste de los derechos de acceso se realizan de acuerdo con el Flujograma Control de Acceso a Sistemas de Información y Administración de Usuarios y Contraseñas.

b. El Proceso de Gestión TICs tendrá en cuenta el reporte de usuarios con sus novedades, enviado por talento humano y secretaría general para validar el acceso a los sistemas de información de la CGN

c. La solicitud de bloqueo del acceso a los sistemas de información de la Contaduría, por vacaciones, permisos temporales, licencias, incapacidades, entre otras novedades administrativas, es responsabilidad de los supervisores de contrato en el caso de los contratistas, y del líder de Talento Humano en el caso de los funcionarios. Estas solicitudes deben ser remitidas al Proceso de Gestión TICs.

14.11. Política de Acceso a los recursos de información

a. Los colaboradores o contratistas deben custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función; conserve bajo su cuidado debe impedir o evitar su sustracción, destrucción, ocultamiento o utilización indebida.

b. Se debe vigilar y salvaguardar los equipos, muebles y bienes que le han sido asignados, y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a los que han sido destinados.

c. El acceso de los usuarios a la red y a los diferentes servicios de red debe permitirse únicamente cuando sea formalmente autorizado por el jefe inmediato.

d. El acceso a los sistemas y recursos de información solamente se debe permitir si existe autorización formal y escrita por parte del jefe inmediato, teniendo en cuenta los siguientes parámetros:

- El jefe inmediato solo puede autorizar acceso a información propia del área que coordina y solo podrá asignar privilegios de acceso a los servidores públicos, contratistas y terceros que están bajo su supervisión.

- En caso de su ausencia o vacancia, el cargo inmediatamente superior en la jerarquía podrá evaluar y autorizar acceso a la información.

e. Es responsabilidad de los servidores públicos, contratistas, terceros y público en general asegurarse de que el acceso y el uso de la información se limite estrictamente a actividades relacionadas con las funciones específicas de la Entidad. Además, se debe garantizar que dicha información sea utilizada siguiendo los criterios de confidencialidad establecidos por la Contaduría General de la Nación.

f. El establecimiento de conexiones directas entre los sistemas de cómputo y comunicaciones de la Contaduría General de la Nación con cualquier otra organización, a través de Internet o cualquier otro tipo de red, debe contar con una evaluación y autorización formal previa, basada en un análisis de riesgos de seguridad por parte del administrador de red o el encargado de la seguridad informática.

g. Módems o dispositivos de índole similar no deben ser utilizados para las comunicaciones de la Contaduría General de la Nación, a menos que un firewall y una red privada virtual sea establecida entre los equipos de cómputo involucrados en dicha comunicación.

h. Una vez se dé por terminada la relación laboral de un servidor público o vínculo contractual de un contratista o tercero, se deben retirar todos los derechos de acceso a los recursos a los cuales estuvo autorizado y se debe realizar también una devolución de activos.

i. La devolución o retiro de equipos, información o software solo debe realizarla el personal autorizado.

14.12. Política de uso de los Recursos de Información

a. Se deben utilizar los bienes y recursos informáticos asignados única y exclusivamente para el desempeño de su empleo, cargo, rol o función. De la misma forma las facultades que lesean atribuidas, o la información reservada a que tenga acceso por razón de su función, debeser utilizada en forma exclusiva para fines de la Entidad.

b. Los sistemas de cómputo entregados por la Contaduría General de la Nación deben ser utilizados únicamente para propósitos propios de la Entidad y son propiedad del Estado, poresta razón se recuerda que el uso que se le dé a los mismos es de carácter oficial.

c. No se pueden almacenar, instalar o utilizar juegos en los equipos de cómputo de laContaduría General de la Nación.

d. Únicamente los funcionarios y técnicos de soporte autorizados por la Contaduría, previa aprobación del Coordinador del GIT de Apoyo Informático, tienen la autorización para instalar y realizar modificaciones en el software y hardware de los equipos de la Contaduría. En este sentido, está estrictamente prohibida la instalación de cualquier software sin la autorización previa del GIT de Apoyo Informático, con el objetivo de asegurar la legalidad y la seguridad de este.

e. Los cambios, ajustes o mejoras en la infraestructura física o lógica de aplicaciones de la Contaduría, deberán ceñirse a las políticas de seguridad de la información de la Entidad.

f. A menos que sean específicamente autorizados por el Coordinador del GIT de Apoyo Informático los servidores públicos de la Contaduría General de la Nación no deben utilizar herramientas de hardware o software que puedan ser empleadas para evaluar vulnerabilidades o comprometer la seguridad de los sistemas de información o la información de otros usuarios. Incidentes que involucren este tipo de

herramientas y el intento no autorizado de comprometer las medidas de seguridad de los sistemas de información, serán considerados como violaciones serias de las políticas de la Contaduría General de la Nación y podrán ser denunciados legalmente.

g. El GIT de apoyo informático, debe realizar un Análisis de Riesgos para el software (aplicativo, sistema operativo) y hardware nuevo, que llegue a la Contaduría General de la Nación.

h. La Contaduría General de la Nación se reserva el derecho de examinar toda la información almacenada en, o transmitida por sus sistemas de cómputo y de comunicación, y debe informar a los servidores públicos, contratistas y terceras partes que no deben esperar privacidad asociada con la información que almacenan o envían a través de estos sistemas.

i. El GIT de Apoyo Informático se encargará de asegurar que todos los usuarios dispongan de una configuración estándar para el uso de los recursos de la Entidad y el acceso a Internet, con el objetivo de garantizar el cumplimiento de lo establecido en esta política. En el caso de los usuarios del aplicativo CHIP que necesiten una configuración particular, esta deberá ser autorizada por la Coordinación del GIT de Apoyo Informático y se registrará como un caso excepcional.

j. El envío de información a través de cualquier medio electrónico, servicio o aplicación (como por ejemplo el sistema de gestión documental o correo electrónico) y que requiera un proceso de autenticación, es decir, usuario y contraseña, será responsabilidad de cada usuario. Lo anterior sustentado en el artículo 55 de la Ley 1437 de 2011 que establece: "Los documentos públicos autorizados o suscritos por medios electrónicos tienen la validez y fuerza probatoria que le confieren a los mismos las disposiciones del Código de Procedimiento Civil".

14.13. Política de Uso del Correo Electrónico

a. Todos los mensajes de correo electrónico deben enviarse mostrando al final el nombre completo, cargo, Proceso o GIT al que pertenece, teléfono, extensión y el nombre de la Entidad.

b. El único servicio de correo electrónico autorizado para el manejo de la información institucional en la CGN es el que cuenta con el dominio contaduria.gov.co.

c. La conexión al correo electrónico y servicios de navegación por Internet son suministrados únicamente para propósitos propios y oficiales de la CGN.

d. Cuando se utilice el correo electrónico para asuntos relacionados con las funciones de la Entidad, debe existir claridad en que algunos puntos de vista expresados pueden ser de los individuos y no representan necesariamente la política de la CGN.

e. Ningún usuario deberá permitir a otro enviar correos utilizando su cuenta.

f. Cuando un servidor público requiere ausentarse de la Entidad por un período superior a 8 días, debe programar el correo electrónico para que automáticamente responda a los remitentes indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia.

g. Antes de enviar un correo deberá verificarse que vaya dirigido a los remitentes interesados.

h. Está prohibida la reproducción y envío de mensajes tipo cadena o similares; ya que puede ocasionar suspensión del servicio temporal o definitivo.

i. La responsabilidad del contenido de los mensajes de correo será del usuario remitente.

j. El contenido de los mensajes de correo se considera confidencial y solo perderá este carácter en casos de investigaciones administrativas, judiciales o incidentes relacionados con seguridad de la información, entendiendo por confidencial aquella información cuyo conocimiento por parte de personas no autorizadas pueda implicar riesgos para la Entidad.

k. No revele sus datos personales, bancarios o contraseñas a través de correos electrónicos y evite hacer clic en los enlaces que se encuentran dentro de los correos que provienen de remitentes desconocidos o direcciones no confiables

l. No se deberá utilizar el correo electrónico institucional como cuenta en redes sociales, ni enviar mensajes para beneficios personales, políticos, avisos clasificados, publicidad comercial o boletines cuya información no guarde relación directa con los intereses de la Entidad. lo anterior aplica también para el manejo de información en las redes

sociales de la CGN

m. Si su cuenta es accedida de manera ilegal por terceros no autorizados, se recomienda cambiar contraseña y denunciar de manera inmediata ante las autoridades competentes, adjuntando la evidencia.
n. Si el funcionario desea acceder a la cuenta de correo institucional desde un dispositivo móvil,deberá aceptar las políticas de seguridad de la Entidad dispuesta para este componente.

o. El correo electrónico institucional en sus mensajes contendrá una nota de confidencialidad, la cual deberá utilizarse siempre en los mensajes.

14.14. Política de red interna de la CGN

La red interna de nuestra institución es un recurso vital que permite la comunicación, el intercambio de información y el acceso a recursos críticos para el desarrollo de nuestras operaciones. Esta política establece las directrices y normativas para el uso seguro, responsable y efectivo de nuestra red interna por parte de todos los empleados y usuarios autorizados.

El propósito de esta política es salvaguardar la integridad, confidencialidad y disponibilidad de los datos, así como proteger los recursos tecnológicos de la institución contra amenazas internas y externas. Es fundamental que todos los usuarios comprendan y sigan estas directrices para garantizar la eficiencia operativa y la seguridad de nuestra red interna.

Esta política es aplicable a todos los empleados, contratistas y terceros que acceden a la red interna de la institución. Se espera que todos los usuarios se adhieran a los principios y prácticas establecidas aquí, y se hace énfasis en la responsabilidad individual en el cumplimiento de estas normativas.

El acceso a la red interna está restringido a empleados y personal autorizados por la institución. Se requiere autenticación para acceder a recursos y datos de la red.

a. Seguridad y Confidencialidad:
Los usuarios son responsables de mantener la confidencialidad y la integridad de la información accesible a través de la red interna. Se prohíbe compartir credenciales de acceso.
b. Uso Aceptable:
El uso de la red interna debe cumplir con las políticas y regulaciones establecidas por la institución. No se permite el acceso a sitios web inapropiados o la descarga de contenido no autorizado.

c. Actualizaciones de Software y Seguridad:
Todos los dispositivos conectados a la red interna deben mantener su software actualizado con los parches de seguridad más recientes. Se promueve el uso de software antivirus y medidas de seguridad adicionales.

d. Respaldo y Recuperación de Datos:
Los datos críticos deben ser respaldados regularmente según los procedimientos establecidos por la institución para asegurar su disponibilidad en caso de pérdida o fallo del sistema.

e. Monitorización y Registro:
La actividad en la red interna puede ser monitoreada y registrada con el fin de asegurar el cumplimiento de las políticas de seguridad y para investigar cualquier actividad sospechosa o incumplimiento de las normativas.

f. Responsabilidades y Consecuencias:
Los usuarios son responsables de su conducta en la red interna. El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo la terminación del acceso a la red y acciones legales según sea necesario.

g. Reducción y Mitigación de Riesgos:
La institución se compromete a identificar, reducir y mitigar los riesgos asociados con el uso de la red interna. Se implementarán controles de seguridad y medidas preventivas para proteger la red contra amenazas conocidas y emergentes. Se fomentará la conciencia sobre seguridad informática y se proporcionará formación regular a los usuarios para mitigar los riesgos de vulnerabilidades y brechas de seguridad.

14.15. Política de Uso del internet

a. Se prohíbe la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados por la CGN.
b. Se prohíbe la descarga, uso, intercambio o instalación de juegos, aplicaciones web de uso personal, redes sociales, música, películas, protectores y fondos de pantalla, software de libre distribución, información o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas que atenten contra la integridad, disponibilidad o confidencialidad de la información de la CGN y sus

partes interesadas.

c. Se prohíbe el acceso a sitios web de contenido para adultos relacionadas con pornografía, drogas, alcohol, violencia, hacking o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
d. Se prohíbe el acceso a sitios web de carácter discriminatorio, racista, o material potencialmente ofensivo, menosprecio o acoso explícito.

14.16. Política de uso de la red inalámbrica pública de la CGN

La presente política establece las directrices a seguir para el acceso y uso apropiado de las zonas establecidas de internet inalámbrico, aplicables a todos los usuarios que utilicen el servicio proporcionado por la Contaduría General de la Nación de acuerdo con las especificaciones definidas en GTI10-POL03 Política para el Uso de la Red Inalámbrica Pública en la CGN.

14.17. Política de acceso a la red privada virtual – VPN

La política de uso de la Red Privada Virtual tiene como objetivo principal, ofrecer a los funcionarios, contratistas y colaboradores una guía sobre las características y requerimientos mínimos que deben ser cumplidos para el uso correcto del servicio de VPN institucional y cualquier mecanismo de acceso remoto a los servicios que provea la Contaduría General de la Nación, como también las implicancias del mal uso. las especificaciones definidas en GTI10-POL01 Política de Acceso a la Red Privada Virtual de la CGN

14.18. Política de Administración de Contraseñas

La presente política establece las directrices para la gestión de las contraseñas de todos los usuario y perfiles que tengan acceso a los recursos de la Contaduría General de la Nación de acuerdo con las especificaciones definidas en GTI02-POL01 Política de Administración de Usuarios y Contraseñas

14.19. Política de criptografía y llaves criptográficas

El proceso de Gestión TICs de la Contaduría General de la Nación ha venido implementando herramientas criptográficas y protocolos autorizados para uso en la Entidad y en los sistemas de información, de tal manera que se utilicen únicamente los recursos autorizados, con el fin de descartar cifrados y protocolos débiles.

a. Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche quehan perdido su confidencialidad. En el caso de los certificados SSL la periodicidad es de uno o dos (2) años, de acuerdo con la disponibilidad presupuestal

b. La administración de llaves criptográficas y certificados digitales está a cargo del proceso Gestión TICs, sin embargo, la administración de tokens bancarios está a cargo del área solicitante, dichos tokens generan una llave dinámica para el acceso a las diferentes plataformas.
c. Los funcionarios o contratistas a quienes les sean asignados tokens físicos, deben almacenarlos bajo llave cuando no los están utilizando o cuando se van a retirar de sus puestos de trabajo.

14.20. Política de Áreas Seguras

La Contaduría General de la Nación cuenta con los siguientes controles para prevenir el acceso no autorizado a las instalaciones de la Entidad, descritos en el flujograma seguridad física y del entorno del procedimiento de seguridad de la información.

a. El ingreso de visitantes al edificio se deberá manejar de acuerdo con los parámetros enmarcados en el manual del usuario del edificio y con el documento: Manual de Seguridad Física, código SF-MA-01.
b. Todas las personas que ingresen al edificio deberán acogerse a los procedimientos de seguridad del edificio, los cuales pueden incluir: arco de detección de metales, detección de armas de fuego, detector de metales manual etc., de acuerdo con el documento: Manual de Seguridad Física, código SF-MA-01.
c. Para el manejo de visitantes en condición de discapacidad la administración del edificio cuenta con un manejo especial, el cual se encuentra enmarcado en lo promulgado por el Estado Colombiano concerniente a generar igualdad, equidad y justicia, de acuerdo con el documento: Manual de Seguridad Física, código SF-MA-01.
d. Una vez el visitante haya pasado el procedimiento de ingreso al edificio, descrito en el literal "a", deberá ingresar al piso 15.
e. El ingreso a las áreas de la Contaduría General de la Nación se hace a través de una puerta de acceso delimitada por la zona de recepción.
f. El acceso de visitantes al Centro de Datos se realiza con acompañamiento de un funcionario del proceso de Gestión TICs, y se deja registro de ingreso y salida en el formato GTI02-FOR01 Bitácora Plataforma Tecnológica, con el fin de dejar rastros de auditoría.
g. El Centro de Datos debe contar con mecanismos que permitan cumplir los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga.
h. La Contaduría General de la Nación cuenta con un plan de emergencias, con el fin de brindar protección contra amenazas externas.
i. El Centro de Datos cuenta con un sistema de detección de incendios

que le permite reaccionar de manera automática ante incendios o humo.

14.21. Política de Áreas Comunes del Edificio

La administración del edificio cuenta con pasos y procedimientos tendientes al control de las zonas comunes del edificio y las cuales la Contaduría General de la Nación deberá adoptar en pro de mantener un alto nivel de control de Seguridad de la Información. De acuerdo con el documento: Manual de Seguridad Física, código SF-MA-01

a. Controlar la permanencia y tránsito de personas y elementos en las áreas comunes y de servicio en los pisos.
b. Velar por el uso correcto de las áreas comunes y de servicio.
c. Reportar cualquier anomalía en el estado de los equipos, señalización y elementos del sistema de emergencia.
d. Cumplir con los procedimientos y consignas entregadas por la administración y el área de seguridad.

14.22. Política de Áreas de Entrega y Carga

La administración del edificio cuenta con procedimientos para el ingreso y entrega de carga, al ser parte de la propiedad horizontal de este edificio, la Contaduría General de la Nación deberá acatar e incluir estos procedimientos dentro de su funcionamiento. De acuerdo con el documento: Manual de Seguridad Física, código SF-MA-01.

a. El proveedor o la persona que trae la carga deberá ser anunciado a la oficina respectiva, con datos completos, nombre, empresa y elementos.

b. De ser autorizado el ingreso, se le informarán los cuidados que debe tener con el ascensor, así como anotar en la planilla de registro de ingreso de carga todos los datos.

c. Si la oficina no autoriza el ingreso de la carga, esta debe ser retirada de inmediato de las zonas establecidas (Recepción – Parqueadero) para dicha entrega.
d. Para el ingreso de carga, solo deberá ser utilizado el ascensor para tal fin, de ninguna maneraeste ascensor estará disponible para visitantes o funcionarios, siempre y cuando no sea autorizado por la administración.

e. Una vez la carga sea dejada en la oficina, las personas que la ingresaron deberán abandonarel piso y dirigirse a la salida.
f. De ninguna manera la Entidad ni el edificio se harán responsables de

carga alguna, por lo tanto, no se podrá guardar elementos a proveedores o personas.

g. Para el ingreso de la carga, este se debe realizar bajo el horario establecido para la utilización del ascensor de carga, por lo tanto, se debe hacer cumplir de acuerdo con el horario de la jornada laboral.
h. Todo el personal de entrega o retiro de carga debe registrarse de acuerdo con el flujograma seguridad física y del entorno del procedimiento de seguridad de la información.
i. El personal de entrega y carga que deba acceder a las áreas de procesamiento de información debe ser autorizado por el líder del proceso y deberá estar supervisado en todo momento por personal de la Contaduría General de la Nación.

j. El material entrante deberá ser inspeccionado para evitar amenazas potenciales como explosivos, productos químicos y otros materiales de riesgo antes de trasladarlo desde el área de carga y entrega hasta su lugar de utilización.

k. El material entrante deberá registrarse de acuerdo con el procedimiento PI-PRC28 Gestión de activos de información.

l. El material entrante deberá inspeccionarse en busca de indicios de manipulación durante su traslado. Si se descubre tal manipulación se deberá informar de inmediato al personal de seguridad.

14.23. Política de Ubicación y protección de los equipos

a. El Centro de Datos de la Contaduría General de la Nación cuenta con sistema de control de acceso, aire acondicionado, sensor de humedad y temperatura, puertas de seguridad con cerradura electromagnética y cierre hermético, sistema de alimentación ininterrumpida (UPS) y corriente regulada.
b. El Centro de Datos está ubicado de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado.

c. Se hace seguimiento a las condiciones (temperatura, humedad, voltaje, y apertura y cierre de puertas) que pueden llegar a afectar los equipos almacenados en el Centro de Datos, con el fin de dar cumplimiento a los requisitos especificados por los fabricantes de los servidores y equipos de comunicaciones que allí se encuentran.

d. Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser

subterráneas o deben estar sujetas a una adecuada protección alternativa (canaletas).

e. En el Centro de Datos los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.

f. En el Centro de Datos se debe contar con la certificación de los puntos de la red para asegurar su adecuado funcionamiento.

g. La implementación de modificaciones, adiciones o de nuevo hardware debe contemplar la revisión de las políticas de seguridad y el formato GTI02- FOR04 Administración de cambios TI.

h. Todos los equipos deben estar completamente probados y aceptados por parte del Proceso Gestión TICs, antes de ser puestos en funcionamiento.

i. Los equipos de cómputo o equipos del Centro de Datos solamente podrán ser dados de baja por el personal autorizado del Proceso Gestión TICs, garantizándose que se han eliminado los riesgos de pérdida de confidencialidad.

j. Los responsables de cada proceso deben aplicar las normas mínimas de seguridad física en las áreas en donde estén instalados hardware, documentación, entre otras.

k. Todo traslado o reasignación de equipos debe ser autorizado y debidamente registrado en el formato GAD22-FOR02 Traslado de elementos devolutivos.

l. Servicios de Suministro: la Entidad cuenta con un sistema de alimentación no interrumpida redundante (UPS) que asegura ante una falla en el suministro de energía, el tiempo necesario de funcionamiento de los servidores, los cuales alojan los sistemas de información. Adicionalmente, el edificio cuenta con una planta eléctrica.

m. Seguridad del Cableado: el Centro de Datos de la Entidad cumple con la normatividad de cableado estructurado y con las características de un Centro de Datos Tier I.

n. Mantenimiento de Equipos: El proceso de Gestión TICs coordina las labores de mantenimiento correctivo y preventivo, las cuales se realizan a través del grupo de soporte y cuando sea necesario será subcontratado dicho servicio, adicional se realiza seguimiento a los

planes anuales de mantenimiento de la infraestructura tecnológica de la Entidad.

14.24. Política de Derechos de Autor

Es política de la Contaduría General de la Nación, el cumplimiento de todas las obligaciones legales, adquiriendo el material patentado de la empresa propietaria o duplicándolo bajo expresa autorización de esta. Todo el software operativo y aplicativo es de propiedad de la Contaduría General de la Nación y solo el grupo de soporte técnico previa autorización del Coordinador del GIT de Apoyo Informático, está autorizado para instalarlo en las estaciones de trabajo de la Entidad.

a. El software patentado es generalmente suministrado bajo un acuerdo de licencia, el cual limita el uso de dichos productos en equipos específicos, y puede limitar las copias únicamente a aquellas con el objetivo de mantener un respaldo de los medios. Por lo tanto, los servidores públicos, contratistas y terceros que trabajan para la Contaduría General de la Nación no deben copiar el software suministrado por la Entidad en medios de almacenamiento, transferir dicho software a otros computadores o suministrar dicho software a terceras partes. Lo anterior aplica para el software desarrollado por la Entidad. La trasgresión de derechos en cierto software, bajo la Ley de derechos de autor, constituye un delito criminal.

b. La Contaduría General de la Nación cuenta con la autoridad y autonomía para realizar auditorías periódicas sobre las estaciones de trabajo, previa autorización del jefe inmediato, para verificar el apropiado uso de software. Se mantendrán los registros de los hallazgos identificados.

c. El supervisor del contrato con terceros hará seguimiento y revisión de los servicios prestados por terceros

d. Se debe cumplir a cabalidad con todas las leyes, normas, decretos, sentencias y demás que sean aplicables.

14.25. Política de Control de Virus

a. La Contaduría General de la Nación es responsable de suministrar un sistema de antivirus el cual debe estar instalado en cada estación de trabajo, equipos portátiles y en los servidores; los usuarios no deben desactivar esta funcionalidad o intentar manipular la configuración en sus equipos.

b. Es responsabilidad de cada usuario utilizar el software para diagnosticar la presencia de virus en la información que provenga de diferentes medios como Internet, memorias USB, archivos compartidos entre otros. Este proceso debe ser realizado antes de abrir o ejecutar los archivos, así como antes de divulgarlos, con el fin de no propagar virus informáticos u otros programas maliciosos al interior de la red.

c. Los sistemas de cómputo que se sospechen han sido comprometidos por virus o software malicioso deben ser apagados y desconectados de la red en forma inmediata. El usuario debesolicitar apoyo técnico e informar al área de soporte técnico del GIT de Apoyo Informático.

d. Todos los medios magnéticos suministrados por un tercero deben ser revisados por el antivirus de la Entidad antes que estos sean utilizados en los computadores personales o servidores de la Entidad.

e. Antes de restaurar archivos desde copias de respaldo, dichas copias deben ser evaluadascon el software antivirus de la Entidad.

14.26. Política de Confidencialidad de la Información

Los siguientes elementos deben ser considerados por los Propietarios de la Información y el GIT de Apoyo Informático, con el objeto de que toda la información de la CGN quede protegida en forma predeterminada:

a. Si la información no está clasificada como pública, ésta no podrá ser proporcionada a ninguna Entidad externa sin un acuerdo de confidencialidad.

b. Los servidores públicos, contratistas y terceros que trabajan para la Contaduría General de la Nación no deben enviar información de carácter diferente a Dominio Público por correo electrónico, a menos de que se tengan medidas adicionales de protección.

c. Toda la información de la Contaduría General de la Nación (publica, publica clasificada y publica reservada) debe estar protegida para evitar que personas no autorizadas la consulten, divulguen o modifiquen sin consentimiento a terceras partes (servidores públicos, prestadores de servicios, entidades externas y personal que realiza alguna actividad dentro de la Entidad). Estas entidades tendrán acceso a la información de la Contaduría General de la Nación únicamente cuando se demuestre la necesidad de conocer su existencia y cuando se haga a través de una cláusula o contrato de confidencialidad.

d. Si se confirma o se sospecha que la información o datos confidenciales o privados, son extraviados o revelados a entidades no autorizadas, el Propietario de la información o quien evidenció el hecho deberá notificar inmediatamente al encargado de la seguridad de información de la Entidad, con el objeto de realizar un control efectivo de posibles daños y tomar las acciones necesarias.

e. Ningún servidor público, contratista o tercero que tenga alguna relación laboral con la Contaduría General de la Nación revelará los controles de seguridad, la forma en que están implementados y las debilidades de los sistemas de información, esto incluye: Información que se proporciona en presentaciones, discusiones, o es tratada en diferentes foros que incluya aspectos técnicos de infraestructura.

f. Toda información clasificada según la Ley 1712 de 2014 debe ser etiquetada (marcada) con base en estándares definidos. Se buscará que estas etiquetas sean mantenidas en buen estado y visibles de tal forma que se puede identificar la clasificación de la información de la Entidad en cualquier momento (Consultar PI28-INS01- Instructivo para la gestión de activos de la información).

g. Cualquier medio de almacenamiento de cómputo que contenga información, deberá ser identificado con una etiqueta.

h. Toda la documentación impresa, escrita a mano o documento legible que contenga información clasificada como publica clasificada y publica reservada, debe tener una etiqueta que indique el nivel apropiado de sensibilidad con base en la clasificación.

14.27. Política de Monitoreo y Evaluación del Cumplimiento

a. El funcionario asignado por el coordinador del GIT de apoyo informático, en primera instancia, tiene la responsabilidad de monitorear las estaciones de trabajo con el fin de identificar lo que pueda ser considerado como software ilegal o aplicaciones que afecten la seguridad de la información.

b. La Contaduría General de la Nación se reserva el derecho de monitorear o inspeccionar en cualquier momento todos los sistemas de información de la Entidad. Esta evaluación puede tener lugar con el consentimiento, presencia o conocimiento del jefe inmediato de los servidores públicos involucrados. Los sistemas de información sujetos a tal examen incluyen, pero no están limitados a: sistemas de archivo de correo electrónico, archivos en discos duros de computadores

personales, archivos en colas de impresión.

c. Debido a que los sistemas de cómputo y comunicaciones suministrados por la Contaduría General de la Nación se emplean únicamente para propósitos de la Entidad, los servidores públicos, contratistas y terceras partes no deben tener expectativas de privacidad asociadascon la información que ellos almacenan o envían a través de estos sistemas de información.

d. El supervisor o el personal técnico asignado a un proceso contractual deberá reportar los incidentes de seguridad de acuerdo con las tareas establecidas para dar cumplimiento a las especificaciones del contrato.

e. El administrador del correo o el Coordinador del GIT de Apoyo Informático no facilitará a otrapersona el contenido de ningún archivo de correo electrónico del personal sin obtener el permiso del usuario o en su defecto, del jefe inmediato, cuando exista un motivo razonable para hacerlo. Dichos motivos pueden incluir, sin limitarse a ello, mantener la integridad del sistema (tal como la eliminación de virus), cumplir obligaciones legales (tal como citaciones judiciales) y efectuar ciertas funciones de administración del sistema (tal como remitir los mensajes con direcciones erróneas).

f. No obstante, la Contaduría General de la Nación puede obtener acceso a la información de los servidores públicos, contratistas y terceros, en caso de que se requiera dicha información para investigaciones o en caso de emergencia. Por ejemplo, si el servidor público, contratistao tercera parte está ausente durante un período prolongado de tiempo debido a enfermedadu otro motivo (previa autorización escrita del jefe inmediato), se podrá tener acceso a la información para suplir necesidades del servicio y para las investigaciones pertinentes.

g. La Contaduría General de la Nación se reserva el derecho de interceptar o vigilar cualquier tráfico de información que pase a través del sistema de la Entidad como parte de sus actividades de vigilancia, mantenimiento, investigación, auditoría o seguridad del desempeño del sistema. Todo el personal debe estar consciente de esto cuando use los sistemas de tecnologías de información de la Entidad.

14.28. Política de Gestión de Incidentes de Seguridad de la Información

a. La Entidad controla el reporte y evaluación de los eventos de

seguridad de la información, tales como: perdida de confidencialidad, integridad y disponibilidad de la información; la respuesta a los incidentes y el aprendizaje obtenido de estos, de acuerdo con el flujograma de Gestión de Incidentes de Seguridad de la Información del procedimiento de seguridad de la información.

b. Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

c. Todo el personal de la Contaduría General de la Nación debe estar vigilante respecto a los incidentes o debilidades de seguridad (incluyendo fallas en el sistema, pérdida del servicio, datos del negocio incompleto o inadecuado, perdida de la confidencialidad). Si se detectan estos incidentes o debilidades de seguridad, deben ser reportados en forma inmediata al encargado de la seguridad de la información al correo electrónico **seguridadinformatica@contaduria.gov.co.**

d. Toda violación de estas políticas se debe notificar inmediatamente al proceso Gestión TICs y al jefe inmediato, de modo que se pueda resolver debidamente el incidente. Con lo anterior se busca reducir los riesgos de seguridad de la información, protegiendo a todas las personas, así como a la Entidad. Así mismo, se deben reportar los eventos de seguridad de la información identificados, de acuerdo con el flujograma gestión de incidentes, amenazas y debilidades del procedimiento de seguridad de la información (GTI-PRC010).

e. Se deben notificar situaciones tales como: personas ajenas a la Contaduría General de la Nación en oficinas y centros de cómputo, correos maliciosos, sospechas de equipos infectados, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso ilegal del software, mal uso de información Corporativa, alteración de información, entre otros.

14.29. Política de Proyectos

Todo proyecto independiente de su naturaleza deberá asegurar que los riesgos de seguridad de la información se identifiquen y gestionen como parte de este; teniendo en cuenta como mínimo los siguientes requerimientos:

a. Establecer los objetivos de seguridad de la información dentro del proyecto

b. Incluir valoración de riesgos de seguridad en cada una de las etapas del proyecto, para identificar los controles necesarios.

c. Garantizar en todas las fases de la metodología de proyectos la aplicación de la seguridad de la información, además de los controles establecidos en la norma ISO 27001.

d. La gestión deberá ser permanente durante el ciclo de vida del proyecto y se deberán asignarlos roles y responsabilidades de dicha labor.

14.30. Política de Pantalla despejada y escritorio limpio

a. Todos los equipos de la CGN son bloqueados automáticamente después de cinco (5) minutos de inactividad por política del directorio activo.

b. Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren de la misma, de forma tal que solo se pueda desbloquear con lacontraseña de usuario

c. Los funcionarios y contratistas de la CGN deben conservar su escritorio físico libre de información escrita o impresa, que pueda ser alcanzada, copiada o utilizada por terceros o personal sin autorización, cada vez que se vayan a retirar de sus puestos de trabajo.

d. En equipos servidores se debe cerrar sesión (log off) si se pretende apagar el equipo o si simplemente se va a dejar desatendido por un periodo de tiempo considerable.

e. Cualquier equipo portátil debe ser debidamente asegurado si se va a dejar desatendido. Es necesario guardarlo bajo llave o utilizar una guaya de seguridad.

f. Se deben utilizar restricciones para los tiempos de conexión en los servidores de la plataforma tecnológica de la CGN, después de un período de tiempo de inactividad el sistema solicitara nuevamente las credenciales.

g. El usuario no debe abandonar su PC, terminal o estación de trabajo sin antes salir de los sistemas o aplicaciones pertinentes o bloquear la estación de trabajo con el comando Windows + L, en teletrabajo con Ctrl+Alt-Fin.

h. Los trabajadores o terceros que tenga dentro de sus funciones la

atención al público deberán almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de los visitantes no autorizados.

i. Las estaciones de trabajo deben apagarse completamente al final de la jornada de trabajo,con la excepción para los casos en los que se haga uso de la VPN (Red Privada Virtual), para lo cual la estación de trabajo deberá permanecer encendida, bloqueada y con la pantalla apagada.
j. Al imprimir información reservada o pública clasificada, los documentos deberán ser retirados de forma inmediata de las impresoras para evitar divulgación no autorizada de la información.
k. Los archivos que contengan información personal sensible deberán ser almacenados en rutas que impidan el fácil acceso por terceros, evitando, por ejemplo, guardarlos en el área de escritorio de la pantalla del computador.
l. La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo losaccesos directos a las aplicaciones necesarias para que los funcionarios o contratistas que ejerzan sus funciones o cumplan sus obligaciones contractuales, según el caso.
m. Los documentos electrónicos que producen los funcionarios o contratistas en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, debenguardarse en la carpeta de almacenamiento en red dispuesta por la Entidad.

14.31. Política de respaldo de datos

La presente política establece las directrices para respaldo de datos en la Contaduría General de la Nación de acuerdo con las especificaciones definidas en GTI03-POL01 Política de Copias de Respaldo.

14.32. Política de Acceso Lógico

La Contaduría General de la Nación cuenta con un control efectivo para el cuidado de la información que reside en los sistemas informáticos de la CGN, la cual establece lineamientos y políticas que restringen el acceso de los usuarios a las aplicaciones y sistemas de la Entidad. Adicionalmente se cuenta con un bloqueo automático de los equipos de cómputo, cuando transcurre un tiempo de inactividad superior a 5 minutos. las especificaciones están definidas en GTI02-POL01- Política de Administración de Usuarios o Contraseñas

14.33. Política de Acceso Físico

El centro de cómputo de la CGN es una zona restringida y cuenta con un control de acceso físico para asegurar que sólo se permita el acceso a personal

autorizado.
Según flujograma de Seguridad física y del entorno.

14.34. Política de Control de Acceso

a. Todos los sistemas conectados a la red de la Contaduría General de la Nación deben solicitar el usuario de acceso a la red y contraseña, la cual tendrá máximo tres (3) intentos fallidos. Sedebe asegurar que información específica como: el nombre de la Entidad, el sistema operativo,el nombre de la aplicación y otros aspectos relevantes no aparezcan hasta que el usuario tenga acceso al sistema.

b. Todos los usuarios deben ser identificados previamente con un usuario de acceso a la red, que será único en el sistema, y una contraseña secreta para poder usar cualquier computadora multi-usuario, servidores, o recursos de sistemas y aplicaciones en producción.

c. Los sistemas no deben permitir sesiones simultáneas con el mismo usuario de acceso a la reddesde diferentes terminales o PC´s.

d. Las novedades (vacaciones, enfermedades, viajes largos, entre otros) de las cuentas de usuario notificadas por los procesos de gestión humana y gestión administrativa, se deshabilitarán de todos los sistemas a los cuáles tienen acceso.

e. Los usuarios deben tener acceso sólo a la información que sea necesaria para el desarrollo de sus actividades y para la cual tengan autorización.

f. El acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro, de acuerdo con los perfiles que se hayan asignado a los usuarios de cada aplicación. Además, sólo los usuarios administradores podrán tener acceso a los sistemas operativos.

g. Se deben revisar al menos cada seis (6) meses los derechos de acceso de los usuarios a losdatos y a los servicios de información, para mantener un control eficaz.

h. El acceso de usuarios remotos debe ser autorizado por el jefe inmediato y el coordinador del GIT de Apoyo Informático, una vez sea diligenciado el formato GTI010-FOR04 - Solicitud de cuentas de usuario institucional - VPN

i. La CGN permitirá las conexiones remotas a los recursos de la plataforma tecnológica; únicamente a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores

desempeñadas.

j. Utilizar la conexión de acceso remoto solo para acceder a servicios (aplicativos e infraestructura) exclusivos de la CGN.
k. La CGN suministrará las herramientas y controles necesarios para realizar conexiones de manera segura.

14.35. Política de Conflictos legales

Las políticas de seguridad de información de la Contaduría General de la Nación fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones. Si algún servidor público o tercero de la Entidad considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, lo debe reportar de forma inmediata al personal encargado de la seguridad de la información de la Entidad o al correo: seguridadinformatica@contaduria.gov.co Así mismo la CGN cumple con todos los requisitos enmarcados en la Ley 1581 de 2012 referente a la protección de datos personales alineándose con la gestión de privacidad de la información.

a. La CGN vela por el cumplimiento de la legislación relacionada con los derechos de autor y propiedad intelectual, para lo cual prohíbe la copia total o parcial de libros, artículo, software, licencias y código fuente u otros elementos diferentes de los permitidos por la ley de derechos de autor.

b. La CGN denunciará cualquier violación a las políticas descritas en este manual, de acuerdo conlo establecido en la ley de delitos informáticos 1273 del 2009 y demás aplicables.

14.36. Política de transferencia de información

a. La transferencia de información deberá realizarse protegiendo la confidencialidad e Integridad de los datos de acuerdo con la clasificación del activo tipo información.

b. Se firmarán actas de confidencialidad con los Servidores públicos o Contratistas que por diferentes razones requieran conocer o intercambiar información clasificada y reservada. Enestos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes del acceso o uso de dicha información.

c. Los Servidores públicos y contratistas deben seguir las indicaciones del Procedimiento de Gestión de Activos de la Información la Entidad, para la transferencia de información de acuerdo con la clasificación

de esta.

d. La transferencia e intercambio de datos e información sensible (información pública clasificada, información pública reservada y sobre todo aquella que contenga datos personales) solamente puede hacerse a través de la red o copiarse a otro medio de almacenamiento, siempre que la confidencialidad e integridad de los datos se garantice.

e. Se deben usar mecanismos criptográficos para garantizar la confidencialidad, integridad y disponibilidad de la información durante su transferencia, de acuerdo con su nivel declasificación.

f. Se debe transferir información únicamente a receptores autorizados, quienes garanticen porescrito el tratamiento de la información que se les vaya a suministrar, por medio de acuerdosde confidencialidad.

g. No se permite el intercambio de información por medios no autorizados por la Entidad.

h. Los emisores deben verificar previamente al envío, el nombre de los destinatarios de la información clasificada como pública reservada, con el fin de reducir la posibilidad de envío de este tipo de datos a destinatarios no deseados.

i. Se prohíbe el envío de archivos que contengan extensiones ejecutables y otras que puedan ser utilizadas para envío de códigos maliciosos, por medio del correo electrónico de la Entidad.

j. Antes de transferir cualquier información, se debe revisar con un software antivirus y antimalware, para garantizar que no esté comprometida con algún código malicioso.

k. Se debe cumplir con los métodos de transferencia de acuerdo con la clasificación de la información, descritos en el instructivo PI28-INS01 Instructivo para la gestión de activos de la información.

14.37. Política de contingencia de los servicios tecnológicos de la CGN

El GIT de Apoyo Informático de la CGN, de manera permanente, identifica y anticipa la pérdida de las capacidades de procesamiento de información que impacten los procesos críticos del negocio, para lo cual actualizará las guías de recuperación de los componentes de la plataforma tecnológica. Las están especificaciones definidas en el Plan de contingencia tecnológica GTI-PLN02.

14.38. Política de Continuidad de negocio de la CGN

La CGN como Entidad rectora responsable de regular la contabilidad general de la nación, con autoridad doctrinaria en materia de interpretación normativa contable, que uniforma, centraliza y consolida la contabilidad pública, hará todo lo que esté a su alcance para asegurar la continuidad de las operaciones y los servicios que presta a las entidades y partes interesadas o grupos de valor, ante una interrupción imprevista de la plataforma tecnológica o un evento catastrófico, de tal forma que se restablezcan en el menor tiempo posible los servicios que soportan los procesos críticos de la Entidad . La Entidad establece como prioridad la preservación de la vida e integridad de sus servidores públicos, contratistas y demás partes interesadas. Las especificaciones están definidas en el Plan de continuidad del negocio de TI GTI-PLN01.

a. En caso de presentarse un incidente de seguridad de la información significativo se deberá gestionar el manejo de la crisis y los mecanismos de comunicación apropiados tanto internos como externos durante el estado de contingencia de conformidad a los lineamientos establecidospor la Entidad.
b. Se establece un programa de pruebas, las cuales deberán ejecutarse de manera que simule lascondiciones de un evento y no se afecte la operación ni los ANS acordados con las partes interesadas. Las pruebas deben ser documentadas y deberán incluir las recomendaciones, planes de acción y lecciones aprendidas respectivas.

14.39. Política Sincronización de relojes

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por la Contaduría General de la Nación deben estar sincronizados con la hora legal colombiana.

14.40. Política Gestión de la vulnerabilidad técnica

a. El proceso Gestión TICs, es responsable de verificar de manera periódica (al menos mensualmente) la información publicada por parte de los fabricantes y foros de seguridad enrelación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la CGN.

b. Se debe generar y ejecutar por lo menos una vez al año un plan de análisis de vulnerabilidades o hacking ético para las plataformas

críticas de la CGN, cuya viabilidad técnica y de administración lo permita.

c. Las acciones correctivas que requieran ser aplicadas en las plataformas tecnológicas, derivadas de la identificación de vulnerabilidades técnicas, son responsabilidad del proceso Gestión TICs, de acuerdo con el formato GTI02-FOR04 administración de Cambios a TI.

14.41. Políticas para proveedores de servicios

Las especificaciones están definidas en la Política de Seguridad para proveedores de servicios GTI10-POL02.

15. Bibliografía

MINTIC, (2021). Política General de Seguridad de la Información. Recuperado el 15 de marzo de 2022 de https://gobiernodigital.mintic.gov.co/692/articles-272947_recurso_1.zip

MINTIC, (2021). Manual de Políticas de Seguridad de la Información. Recuperado el 15 de marzo de 2022 de https://gobiernodigital.mintic.gov.co/692/articles-272946_recurso_1.zip

ISO/IEC 27001:2013, Information Technology. Security Techniques. Code of Practice for Information Security Controls.

ISO/IEC 27002:2013, Information Technology. Security Techniques. Code of Practice for Information Security Controls.

REVISADO POR:	APROBADO POR:
LIDER DE PROCESO GESTIÓN TIC´S	**REPRESENTANTE DE LA DIRECCION COORDINADOR GIT DE PLANEACION**