SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
10/10/2025	GTI-POL00	01	**1** de **44**

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

OCTUBRE DE 2025

CONTROL DE CAMBIOS

VERSIÓN	SECCIÓN	TIPO	FECHA (DD/MM/ AAAA)	AUTOR	OBSERVACIONES
1.0	Todas	Creación	15/8/2024	GIT de Apoyo Informático	Creación del documento tomando como base el GTI-MAN01 Manual de Seguridad de la Información y Digital V.6, registrando la política general y políticas específicas de seguridad de la información y ajustando el nombre del documento. Nota: El formato anterior no incluyó tabla de control de cambios. Aprobado el 30/10/2024 en CIGD
2.0	Todas	Actualización	21/7/2025	GIT de Apoyo Informático	Se realiza actualización e incorporación de los nuevos controles de la norma ISO/IEC 27001:2022, verificando cada uno de los controles Vs las políticas para dar cumplimiento. Creación de Política de Inteligencia de Amenazas, Política para uso de servicios en la nube Aprobación: CIGD 10 de octubre de 2025.

CONTENIDO

1. INTRODUCCIÓN 5
2. OBJETIVO 5
3. ALCANCE 5
4. DEFINICIONES 5
5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 6
6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL 6
7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL 6
7.1. Política de Seguridad de la Información en la Gestión de Proyectos 7
7.2. Política de Dispositivos de punto final de usuario (BYOD: *Bring Your Own Device*) 7
7.3. Política de Teletrabajo y Trabajo Remoto 9
7.4. Política para el Talento Humano 10
7.5. Política de Capacitación y Entrenamiento en Seguridad de la Información y Seguridad Digital 11
7.6. Política de Procesos Disciplinarios 11
7.7. Política de Uso de los Recursos de Información 11
7.8. Política de Uso del Correo Electrónico 13
7.9. Política de Uso del Internet 14
7.10. Política de Gestión de Activos 15
7.11. Política de Inteligencia de Amenazas 17
7.12. Política de Clasificación de la Información 19
7.13. Política de Control de Acceso 20
7.14. Política de la Red Interna LAN (Network Access) 22
7.15. Política de Uso de la Red Inalámbrica Pública WLAN 23

7.16. Política de Acceso a la Red Privada Virtual (VPN) 23
7.17. Política de Administración de Usuarios y Contraseñas 24
7.18. Política de Confidencialidad de la Información 25
7.19. Política de Criptografía y Llaves Criptográficas 26
7.20. Política de Acceso Físico 27
7.21. Política de Áreas Seguras 27
7.22. Política de Ubicación y Protección de los Equipos 28
7.23. Política para el Uso de Medios Removibles, Borrado Seguro y Disposición de Medios 30
7.24. Política de Pantalla Despejada y Escritorio Limpio 31
7.25. Política de Control de Virus o software malicioso 32
7.26. Política de Respaldo y restauración de Datos 33
7.27. Política de Sincronización de Relojes de los sistemas 35
7.28. Política de Gestión de la Vulnerabilidad Técnica 35
7.29. Política de Transferencia de Información 36
7.30. Política para Desarrollo y Mantenimiento de Software 37
7.31. Políticas para Proveedores de Servicios 38
7.32. Política de Gestión de eventos e incidentes de Seguridad de la Información 38
7.33. Política para uso de servicios en la nube 39
7.34. Política de Continuidad de Negocio 40
7.35. Política de Contingencia de los Servicios Tecnológicos 41
7.36. Política de Protección de los Derechos de Autor 41
7.37. Política de Conflictos Legales 42
7.38. Política de Monitoreo y Evaluación del Cumplimiento 43
8. Bibliografía 44

1. INTRODUCCIÓN

Este documento describe la política general y las políticas específicas de seguridad de la información y seguridad digital de la Contaduría General de la Nación (CGN); para su elaboración, se toman como base los controles y requisitos identificados en el estándar ISO/IEC 27001 y el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC).

Las presentes políticas constituyen parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y se convierten en la base para la implementación de procedimientos, controles y buenas prácticas de seguridad de la información y seguridad digital.

2. OBJETIVO

Establecer lineamientos claros que deben seguir todos los servidores públicos y colaboradores que tenga acceso a los recursos tecnológicos y digitales de la CGN, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información y fortalecer la continuidad de las actividades misionales, administrativas, operativas y logísticas de la entidad, promoviendo el uso seguro de los activos de información, reduciendo los riesgos y optimizando la inversión en tecnologías de información.

3. ALCANCE

Este documento aplica a todos los activos de información o cuya administración o custodia esté a cargo de la CGN, en cuyo caso es responsabilidad de todos los servidores públicos, colaboradores y terceros que tengan algún tipo de vinculo contractual o convenio con la CGN conocer y cumplir las siguientes políticas con el fin de usar los recursos tecnológicos de manera responsable y segura.

4. DEFINICIONES

Las definiciones relacionadas con seguridad de la información, seguridad digital, ciberseguridad y protección de datos personales se encuentran unificadas en el documento GTI-MAN02 Manual de Términos y Definiciones de Seguridad de la Información y Seguridad Digital.

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El Sistema de Gestión de Seguridad de la Información, en adelante SGSI presenta las directrices y lineamientos definidos para establecer, implementar, mantener y mejorar continuamente, acorde con los requisitos de la Norma NTC-ISO/IEC 27001:2022 especificados en el **Manual del sistema de gestión de seguridad de la información y seguridad digital – GTI-MAN01**

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

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

Por lo anterior, la CGN implementa estrategias y controles lógicos, físicos y digitales en el marco de un Sistema de Gestión de Seguridad de la Información (SGSI), alineado con la Norma ISO/IEC 27001. Estas acciones buscan proteger la infraestructura crítica que respalda los procesos misionales, garantizando la disponibilidad de los recursos necesarios y adoptando un enfoque integral basado en la gestión de riesgos, la atención de incidentes de seguridad de la información y la mejora continua del SGSI.

En cumplimiento de lo dispuesto, la CGN se compromete a garantizar, verificar y dar estricto cumplimiento a los requisitos legales, reglamentarios, regulatorios, contractuales y de gestión documental, orientados a la mejora continua, a la eficacia del SGSI y al logro de los objetivos de seguridad de la información definidos por la Alta Dirección.

7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

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

7.1. Política de 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 de proyectos, cuando aplique.

b. Valorar y hacer seguimiento a los riesgos y controles aplicados durante todas las fases del proyecto.

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

7.2. Política de Dispositivos de punto final de usuario (BYOD: ***Bring Your Own Device***)

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

a. Para la utilización de los dispositivos móviles se debe cumplir con las políticas:
   - *GTI10-POL01 Política de Acceso a la Red Privada Virtual de la CGN*
   - *GTI10-POL03 Política para el Uso de la Red Inalámbrica Pública en la CGN*

b. Los portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Se les debe proporcionar una forma apropiada de protección al acceso (por ejemplo: contraseñas de encendido, encriptación, etc.) con el fin de prevenir un acceso no autorizado.

c. Las instrucciones del fabricante concernientes a la protección del equipo se deben seguir en todo momento (por ejemplo: para protegerse contra la exposición de campos electromagnéticos muy fuertes).

d. Los equipos de cómputo, así como la información almacenada en los mismos, son propiedad de la CGN, 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.

e. 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 servidor público o colaborador que lo tenga asignado.

f. Solo se podrán utilizar dispositivos provistos por la entidad con sistemas operativos, sistema de antivirus y aplicaciones aprobadas para el cumplimiento de las obligaciones / funciones de los colaboradores.

g. Los dispositivos móviles deben ser actualizados con sus parches de seguridad y últimas versiones, generadas por los proveedores, en las distintas aplicaciones.

h. El acceso a los dispositivos móviles debe realizarse por medio de usuario y contraseña debidamente registrado en el controlador de dominio.

i. Está prohibido el uso compartido de dispositivos sin control de acceso individual. Para que otro usuario distinto al asignado al equipo de cómputo pueda utilizar el equipo debe cerrar la sesión del actual usuario e iniciar una nueva sesión con su usuario y contraseña.

j. Todo incidente relacionado con pérdida, robo o acceso indebido desde dispositivos móviles deberá reportarse a la Mesa de Servicios.

k. El servidor público o colaborador que utilice equipos de cómputo de su propiedad para el desarrollo de sus funciones o compromisos será responsable de:

- Usar software legal instalado en el equipo.
- Contar con software de protección de antivirus licenciado.
- Uso de VPN establecido por la CGN.
- Segregar la información personal e institucional, para el caso de la institucional colocarla en la herramienta de almacenamiento de nube autorizada por la CGN.

- 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.
- La entidad se reserva el derecho de desactivar el licenciamiento de propiedad de la CGN, así como, eliminar los datos institucionales ante eventos de pérdida, robo o desvinculación.
- Mantener actualizado con las últimas versiones del producto y parches de seguridad.

La CGN se reserva el derecho de determinar cuándo un equipo personal no puede ser utilizado para acceso a los servicios de TI o tecnológicos de la entidad.

7.3. Política de Teletrabajo y Trabajo Remoto

La CGN establece los lineamientos de teletrabajo en la Resolución 003 de 2025, por la cual se adopta la modalidad de teletrabajo suplementario como modalidad de teletrabajo y la Resolución 455 de 2024 por la cual se adopta el procedimiento interno de trabajo en casa, donde se establecen los mecanismos de adopción, modalidad y obligaciones generales de los servidores públicos o colaboradores.

Los servidores públicos o colaboradores en la modalidad de teletrabajo o trabajo remoto deben cumplir con las siguientes directrices:

a. Hacer uso adecuado y exclusivo de los recursos tecnológicos informáticos aprobados para el cumplimiento de las funciones o actividades asignadas.
b. Usar software legal instalado en el equipo.
c. Contar con software antivirus licenciado y actualizado.
d. Mantener actualizado el sistema operativo y las aplicaciones.
e. Establecer comunicación segura mediante el uso de canales VPN establecidos por el GIT de Apoyo Informático.
f. De contar con equipo remoto asignado por la CGN y accesible vía escritorio remoto, abstenerse de instalar software o programas ejecutables en los equipos asignados sin previa autorización del GIT de Apoyo Informático, el cual se reserva el derecho de verificar la necesidad y las implicaciones de seguridad de su instalación.
g. Está prohibido el envío de archivos con información institucional por medios no oficiales, tales como Dropbox, WeTransfer, correos de dominio diferente a contaduría.gov.co, etc.

h. La sesión establecida con la CGN por medio de VPN o al dominio contaduría.gov.co por medio de las herramientas colaborativas no debe ser utilizada por una persona diferente al servidor público o colaborador autorizado.

i. No deben establecerse conexiones desde un sitio de acceso público como un café internet, un aeropuerto o un restaurante, entre otros.

j. Sin excepción no se debe establecer conectividad con un equipo de cómputo virtual o físico diferente al asignado o autorizado para teletrabajo o trabajo remoto.

k. Reportar cualquier evento anormal aplicando el Procedimiento de Gestión de Incidentes de Seguridad de la Información y Seguridad Digital.

l. La CGN se reserva el derecho de monitorear el registro de la conexión establecida en modalidad de teletrabajo o trabajo remoto.

m. Respecto a la protección del entorno de trabajo, el colaborador debe evitar realizar actividades laborales en lugares públicos o compartidos sin medidas de protección física (pantallas de privacidad, auriculares, etc.).

n. La información institucional no debe almacenarse permanentemente en dispositivos personales, debe almacenarse en medios autorizados (repositorios corporativos o nube institucional).

o. La CGN se reserva el derecho de determinar cuándo un equipo personal no puede ser utilizado para trabajo remoto o teletrabajo.

7.4. Política para el Talento Humano

La CGN establece los lineamientos de los procesos de selección, vinculación, cambio de empleo o desvinculación del personal así:

a. Planta: las especificaciones están definidas en los documentos *GTH-PRC19 Selección y vinculación de personal de planta* y *GTH-PRC20 Desvinculación del personal de planta.*

b. Contratistas: Las especificaciones están definidas en los documentos *GAD-MAN01 Manual de contratación* y *GAD-INS01 Instructivo Contratación Directa-Prestación de Servicios Profesionales*.

Las responsabilidades y los deberes de seguridad de la información que se deben dar durante y después de los procesos de selección, vinculación, cambio de empleo o desvinculación del personal se especifican en:

Los documentos *MAN01-FOR31 Acuerdo de confidencialidad y aceptación de las políticas de la seguridad de la información* a mantener la confidencialidad de la información durante y después en caso de retiro y en el Formato GTI10-FOR09 Gestión De Cuentas De Usuario.

7.5. Política de Capacitación y Entrenamiento en Seguridad de la Información y Seguridad Digital

a. La CGN, en cabeza del oficial de seguridad de la información, o quien haga sus veces, realizará actividades de inducción, reinducción y capacitaciones (internas y externas) a servidores públicos y colaboradores con el fin de asegurar el conocimiento, uso y cumplimiento de las políticas de seguridad de la información de la CGN.

b. La CGN, en cabeza del Oficial de seguridad de la información, o quien haga sus veces, elaborará propuestas de piezas gráficas mensuales para divulgar temas relacionados con seguridad de la información.

c. Los temas principales se enmarcan en la apropiación de los controles propuestos en el Anexo A de la Norma NTC ISO/IEC 27001.

7.6. Política de Procesos Disciplinarios

En caso de una violación a la seguridad de la información, la CGN cuenta con un proceso formal, de acuerdo con la Ley 1952 de 2019 - Principios y normas rectoras de la ley disciplinaria, modificada por la Ley 2094 de 2021, aplicada por parte de Secretaría General.

7.7. 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 le sean atribuidas o la información reservada a la que tenga acceso por razón de su función, debe ser utilizada en forma exclusiva para fines de la entidad.

b. Los sistemas de cómputo y en general los servicios de TI y tecnológicos dispuestos por la CGN deben ser utilizados únicamente para propósitos propios de la entidad y son propiedad del Estado, por esta razón el uso que se le dé es de carácter oficial.

c. No se puede descargar desde internet, almacenar, instalar o utilizar juegos, música y en general cualquier tipo de archivo o software no autorizado de acuerdo con los criterios definidos, en los equipos de cómputo, servicios de almacenamiento y carpetas compartidas de la CGN.

d. Únicamente los servidores públicos y/o colaboradores de soporte autorizados por la CGN, tienen la autorización para instalar y realizar modificaciones en el software y hardware de los equipos de la CGN atendiendo las políticas aquí definidas. 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 CGN deberán dar cumplimiento a las políticas de seguridad de la información de la entidad.

f. Solamente los usuarios del GIT de apoyo Informático en cumplimiento de sus obligaciones pueden utilizar herramientas de hardware o software que puedan ser empleadas para evaluar vulnerabilidades. Los demás servidores públicos o colaboradores de la CGN no deben utilizar herramientas de software o hardware que comprometan 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 y en general de los servicios de TI y tecnológicos serán considerados como violaciones serias de las políticas de la CGN y podrán ser denunciados legalmente.

g. El GIT de Apoyo Informático debe adquirir software y hardware legal o de código abierto que satisfaga las necesidades de la CGN.

h. El GIT de Apoyo Informático se encargará de asegurar que todos los usuarios dispongan de una configuración estándar a nivel de seguridad perimetral, red y acceso a Internet para el uso de los recursos tecnológicos de la entidad.

i. El envío de información a través de cualquier medio electrónico, servicio o aplicación (como por ejemplo el sistema de gestión documental o el correo electrónico) 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".

7.8. 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.

a. Se prohíbe el uso del correo institucional con el dominio contaduria.gov.co para fines personales o no relacionados con las actividades de la organización.

b. 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.

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

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

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

f. Está prohibida la reproducción y envío de mensajes tipo cadena o similares.

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

a. Está prohibido reenviar información catalogada como restringida, reservada o confidencial a cuentas de correo personales o externas sin autorización previa, la cual solo perderá este carácter, en casos de investigaciones administrativas, judiciales o incidentes relacionados con seguridad de la información, por implicar riesgos para la entidad

b. 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.

c. 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.

d. Si su cuenta es accedida de manera ilegal por terceros no autorizados, se deberá cambiar la contraseña inmediatamente y reportar a los correos institucionales seguridadinformatica@contaduria.gov.co y mesadeservicio@contaduria.gov.co, adjuntando la evidencia.

e. Si el servidor público o colaborador desea acceder a la cuenta de correo institucional desde un dispositivo móvil, deberá aceptar las políticas de seguridad de la entidad.

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

g. La autenticación para acceder al correo electrónico se debe realizar con el control de doble factor de autenticación (2FA).

7.9. Política de Uso del Internet

a. Se prohíbe la descarga de software desde internet, así como su instalación en los equipos de cómputo, las estaciones de trabajo o dispositivos móviles asignados por la CGN.

b. Se prohíbe la descarga, uso, intercambio o instalación de juegos, juegos y apuestas en línea, envío de correos electrónicos masivos (spam) aplicaciones web de uso personal, redes sociales, música, películas, protectores y fondos de pantalla, software de libre distribución, servicios P2P, información o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, así como 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 ilegal, violento, discriminatorio, racista, o material potencialmente ofensivo, o relacionado con situaciones de menosprecio o acoso implícito o que infrinja los derechos de autor
e. El uso del servicio de Internet es solamente con fines laborales, se prohíbe para fines personales
f. La navegación en sitios web será previamente permitida por medio de filtros de contenidos web mediante la plataforma de seguridad perimetral.
g. Se exige el uso de navegadores actualizados y con protección activa contra malware y phishing.

7.10. Política de Gestión de Activos

a. Inventario de activos: el Oficial de Seguridad y Privacidad de la Información, o quien haga sus veces, velará por que los líderes de procesos anualmente identifiquen y documenten el inventario de activos de información, siguiendo las indicaciones del procedimiento GTI-PRC12 - Gestión de activos de información.

b. Uso aceptable de la información y otros activos asociados:

1. La información (física y digital), los sistemas de información, aplicaciones, servicios de TI, servicios tecnológicos y en general el hardware y software) propiedad de la CGN son activos de la entidad y se proporcionan a los servidores públicos o colaboradores autorizados para cumplir con los propósitos de la entidad.
2. La información será etiquetada y deberá dar un manejo adecuado según su clasificación, siguiendo las directrices del *Procedimiento de gestión de activos la información* (GTI-PRC12), el *Instructivo de gestión de activos de información* (GTI12-INS01) y el formato *Inventario de activos de información* (GTI12-FOR01).
3. El hardware y software que son adquiridos por la entidad deberán etiquetarse con número de inventario en el área de almacén antes de que sean asignados.
4. Una vez se dé por terminada la relación laboral de un servidor público o vínculo contractual de un colaborador, o cuando se realice el traslado

de área, se debe gestionar la devolución de los activos asignados mediante el formato GTI11-FOR02-*Salida y reintegro de elementos*.

5. Los recursos de información de la CGN solo pueden ser utilizados para fines relacionados con el desarrollo de las actividades laborales y los objetivos institucionales.
6. Los recursos de información y servicios colaborativos deben utilizarse de manera responsable, exclusivamente para almacenar y compartir información relacionada con la CGN.
7. Los servidores públicos, contratistas y proveedores que tengan acceso a la información institucional, deben cumplir con los requisitos exigidos por la CGN.
8. Los servidores públicos, contratistas, proveedores y otros, que tengan acceso a la información institucional deben respetar la privacidad de la información de la CGN y no divulgar información confidencial o sensible a terceros no autorizados. Se deben seguir los lineamientos y procedimientos establecidos para el manejo y protección de la información confidencial.
9. La CGN se reserva el derecho de monitorear y auditar el uso de los recursos de información para asegurar el cumplimiento de esta política y para garantizar la seguridad de la información. Los usuarios deben estar conscientes de que el uso de los recursos puede ser monitoreados y registrados.
10. Los servidores públicos o colaboradores deben custodiar y cuidar la documentación e información física y/o digital que, por razón de su empleo, cargo o función, conserve bajo su cuidado.
11. No se deben reutilizar documentos para impresión con datos personales, o documentos catalogados como públicos reservados o públicos restringidos.
12. No se deben dejar desatendidos y sin ningún control de acceso documentos físicos, medios de almacenamiento externo (USB, discos duros, SD Card, CD, entre otros), Tokens y otros activos de información en los puestos de trabajo, oficinas, salas de reuniones, viajes o lugares de acceso público. Los computadores portátiles se deben llevar como equipaje de mano.
13. La CGN brinda a través de los servicios colaborativos versiones de los archivos trabajados, las copias temporales y/o permanentes de

información en los siguientes 3 niveles: La información documental tendrá su respaldo en la nube durante la ejecución del contrato o su relación laboral y al finalizar se conservará durante 90 días en la nube; pasado este tiempo se realizará el traslado a un almacenamiento local durante 2 años. Posterior a lo anterior la información se eliminará permanentemente.

14. Se debe realizar de forma segura la eliminación de información de acuerdo con el instructivo GTI010-INS01 Instructivo borrado seguro.
15. Los activos tecnológicos deben mantenerse operativos mediante procesos de mantenimiento preventivo y actualización.
16. Todos los dispositivos de la plataforma tecnológica deben mantener su software actualizado con los parches de seguridad más recientes.
17. Se deberán implementar controles contra accesos no autorizados, malware y pérdida de información en los diferentes activos de información.
18. Al final de su vida útil, los activos deben ser tratados conforme al procedimiento de eliminación segura, evitando cualquier recuperación no autorizada de información.
19. Mantener la política de respaldo y restauración de información actualizada y realizar los respaldos de información de los activos de información en operación.

7.11. Política de Inteligencia de Amenazas

La CGN establece los lineamientos para la prevención, detección y respuesta a software malicioso (malware) en los sistemas de información y activos tecnológicos de la entidad, para todos los empleados, contratistas, proveedores y cualquier otra entidad que tenga acceso a los mismos, tomando las medidas de seguridad efectivas para proteger la confidencialidad, integridad y disponibilidad de la información.

Cubre todas las actividades relacionadas con la inteligencia de amenazas incluyendo la recopilación de información de los dispositivos, redes, aplicaciones y demás componentes, para el análisis, la difusión y la toma de decisiones basadas en la inteligencia obtenida.

En la CGN se cuenta con las siguientes fuentes de inteligencia de amenazas para recopilar y analizar información que nos permite anticiparnos y protegernos eficazmente contra las amenazas:

Antivirus ESET Protect

Es la solución de antivirus, diseñada para proteger los activos de la CGN contra software malicioso. Esta herramienta nos permite detectar amenazas de forma temprana, reducir el tiempo de respuesta y mejorar la seguridad general de la infraestructura.

La herramienta nos brinda inteligencia de amenazas para detección en tiempo real, análisis heurístico y actualizaciones constantes, ofreciendo protección proactiva contra malware y análisis de archivos sospechosos en un entorno seguro. Además, ofrece capacidades de respuesta ante incidentes, lo que nos permite mitigar los riesgos de manera proactiva.

Cuenta con una consola unificada para equipos de cómputo físicos, virtuales y servidores Windows, con alertas y reportes.

Monitoreo: Se basa en el mantenimiento de las medidas de protección contra software malicioso en los activos de información de la CGN

Correo GMAIL

Es el servicio de correo electrónico brindado por Google con cuentas institucionales de la CGN, que incluye funciones avanzadas de seguridad como chequeo de archivos adjuntos, verificación de software malicioso y spam para fortalecer la autenticación, integridad y confiabilidad del correo electrónico, utilizando:

1. Protocolos SPF (Sender Policy Framework) que permite validar servidores autorizados para enviar correos en nombre del dominio contaduria.gov.co
2. DKIM (Domainkeys Identified Mail) garantiza la integridad de los mensajes a través de firmas criptográficas que evitan la manipulación en tránsito
3. DMARC (Domain-based Message Authentication, Reporting and Conformance) fuente que orquesta para generar políticas para la detección proactiva frente ataques de suplantación, phishing u otra amenaza y generar informes.

Monitoreo: Análisis de mensajes para detectar phishing, malware o enlaces

maliciosos, clasificación y envío a la carpeta de Spam de mensajes sospechosos, bloqueo de archivos adjuntos potencialmente peligrosos, soporte para autenticación en dos pasos (2FA)

Firewall Fortinet

Es un dispositivo de seguridad que protege redes y sistemas contra amenazas internas y externas, controlando el tráfico que entra y sale, brindando:

1. Control de tráfico y filtrado para bloquear o limitar conexiones según políticas de seguridad.
2. Prevención de intrusiones (IPS): Detecta y bloquea ataques, exploits y amenazas en tiempo real.
3. Inspección profunda (DPI): Analiza el contenido del tráfico, incluso si está cifrado (HTTPS/SSL).
4. Protección contra malware y ransomware: Usa inteligencia global (FortiGuard) para detectar archivos y sitios maliciosos.
5. Control de aplicaciones: Identifica y gestiona el uso de aplicaciones en la red.
6. VPN segura: Crea túneles cifrados para el acceso remoto de usuarios y sedes.
7. Filtrado web y antiphishing: Bloquea sitios maliciosos, de phishing o con contenido no autorizado.

Monitoreo: Análisis de tráfico de red (entrante/saliente y conexiones sospechosas, eventos de seguridad (intrusiones, malware, bloqueos), Conexiones VPN y accesos remotos.

7.12. Política de Clasificación de la Información

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

- Pública: información que puede ser divulgada al público en general sin restricciones y no causa prejuicio a la entidad.
- 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.

- Pública Restringida: información pública que no debe ser divulgada debido a que esto puede causar daño a intereses públicos.

Toda información clasificada deberá ser etiquetada en su formato físico o digital, de manera clara y visible, utilizando un estándar de marcado definidos para asegurar su correcto manejo.

La información clasificada debe almacenarse en medios seguros, transmitirse por canales físicos o digitales protegidos, y su acceso debe estar restringido según el principio de menor privilegio. Además, debe ser respaldada mediante copias de seguridad.

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

7.13. Política de Control de Acceso

a. El acceso de los usuarios a los servicios de TI y servicios tecnológicos debe permitirse únicamente cuando sea formalmente autorizado por el jefe inmediato y gestionado por el GIT de Apoyo Informático.

b. Todos los servicios de TI y servicios tecnológicos conectados deben solicitar el usuario de acceso y contraseña, la cual tendrá un máximo de intentos fallidos.

c. 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 dispositivo móvil, servidores o recursos de sistemas y en general cualquier servicio de TI y servicio tecnológico.

d. Las novedades como vacaciones, incapacidades, viajes prolongados, entre otras, reportadas por los procesos de Gestión Humana y Gestión Administrativa, serán motivo para la deshabilitación de las cuentas de usuario en el Directorio Activo, lo que implicará la suspensión del acceso a todos los servicios de TI y recursos tecnológicos asociados.

e. Los usuarios deben tener acceso solo a los servicios de TI y tecnológicos que sean necesarios para el desarrollo de sus actividades y para la cual tengan autorización.

f. El acceso a los servicios de TI y tecnológicos se debe basar en el principio de menor privilegio, y asignar roles en función de su responsabilidad.

Además, solo los usuarios administradores podrán tener acceso a los sistemas operativos.

g. Se deben revisar al menos una vez al año, los derechos de acceso de los usuarios para mantener un control eficaz.

h. El acceso de usuarios remotos debe ser autorizado por el jefe inmediato, una vez sea diligenciado el formato *GTI010-FOR09* ***- Gestión de cuentas de usuario.***

i. La CGN permitirá las conexiones remotas a los recursos de la plataforma tecnológica únicamente a servidores públicos o colaboradores autorizados y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

j. Se deberá utilizar la conexión de acceso remoto solo para acceder a servicios de TI y tecnológicos exclusivos de la CGN.

k. La CGN suministrará las herramientas y controles necesarios para realizar conexiones remotas de manera segura.

l. Una vez se dé por terminada la relación laboral de un servidor público o vínculo contractual de un colaborador, se deben retirar todos los derechos de acceso a los servicios de TI y tecnológicos a los cuales estuvo autorizado y se debe realizar también una devolución de activos.

m. La devolución o retiro de equipos, información o software solo debe realizarla el personal autorizado del GIT de Apoyo Informático.

n. Las cuentas de usuario deben ser únicas, personales e intransferibles, así como la creación, modificación y eliminación de cuentas debe ser solicitada formalmente y registrada en los formatos definidos.

o. Se deberá aplicar autenticación de doble factor o multifactorial en los servicios de TI y tecnológicos que se consideren críticos y que cuente con los recursos tecnológicos para su implementación. Las contraseñas de acceso deben cumplir con los lineamientos de la *GTI02-POL01 Política de Administración de Usuarios y Contraseñas*.

p. Aplicar técnicas de enmascaramiento de datos, fortaleciendo el acceso a la aplicación misional, mediante la sustitución de datos sensibles, usando algoritmos de encriptación.

q. Aplicar mecanismos de cifrado en los procesos de autenticación y control de acceso que garanticen que ninguna contraseña, token o certificado sea expuesto en texto plano.

7.14. Política de la Red Interna LAN (Network Access)

La red interna de la CGN es un recurso vital que permite la comunicación, el intercambio de información y el acceso a los servicios de TI y tecnológicos para el desarrollo de las operaciones. Esta política establece las directrices y normativas para el uso seguro, responsable y efectivo de la red interna por parte de todos los servidores públicos y colaboradores autorizados.

a. Para el acceso a la red interna se requiere autenticación y está restringido a servidores públicos o colaboradores autorizados por la entidad.
b. Todos los dispositivos de la plataforma tecnológica deben mantener su software actualizado con los parches de seguridad más recientes.
c. 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.
d. 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 políticas.
e. 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.
f. 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.
g. La red LAN debe estar segmentada por funciones utilizando VLAN y reglas para restringir el tráfico entre las distintas zonas (usuarios, servidores, procesos, DMZ datos, etc.)
h. El acceso a la red cableada se otorgará solo a dispositivos autorizados mediante autenticación MAC en conjunto con puerto seguro.
i. Es necesario el uso de protocolos seguros HTTPS para la transmisión de información.

j. La intercepción de tráfico de red solo está autorizada para el GIT de Apoyo Informático.

7.15. Política de Uso de la Red Inalámbrica Pública WLAN

Define los lineamientos para el uso del internet inalámbrico público en la CGN. Las especificaciones están definidas en el documento *GTI10-POL03 Política para el Uso de la Red Inalámbrica Pública en la CGN*.

Las redes inalámbricas deben estar cifradas con WPA2-Enterprise o WPA3.

La red WLAN destinada a visitantes debe estar lógicamente segregada de la red institucional, con acceso restringido únicamente a servicios de internet. El acceso será de carácter temporal y debidamente registrado.

7.16. 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 servidores públicos y colaboradores una guía sobre las características y requerimientos mínimos que deben ser cumplidos para el uso correcto del servicio de la VPN institucional y cualquier mecanismo de acceso remoto a los servicios que provea la CGN como también las implicaciones del mal uso.

Solo los usuarios registrados y autorizados podrán establecer conexiones VPN a los servicios de TI y Tecnológicos de la CGN.

Toda conexión VPN deberá requerir doble factor de autenticación: contraseña institucional más un segundo factor (token, aplicación de autenticación, SMS, etc.).

El acceso por VPN deberá realizarse exclusivamente desde dispositivos personales BYOD o de la CGN autorizados, con antivirus, parches de seguridad del sistema operativo actualizados y configuraciones de seguridad definidas por la CGN.

Se prohíbe el uso de la conexión VPN para fines personales, navegación no institucional, o descargar software sin autorización.

Solo se debe utilizar para el acceso los servicios de TI y tecnológicos necesarios

para el cumplimiento de funciones laborales.

Toda conexión VPN deberá utilizar protocolos de cifrado. El túnel VPN debe proteger toda la comunicación entre el dispositivo del usuario y los recursos tecnológicos internos de la CGN.

Todas las sesiones VPN deben ser registradas en la plataforma de seguridad de la entidad y monitoreadas para detectar conexiones anómalas o no autorizadas.

Las sesiones VPN se cerrarán automáticamente tras cierto tiempo de inactividad o una duración máxima.

Los accesos VPN se revisarán periódicamente y se revocarán los no justificados o vencidos.

El uso indebido o no autorizado de la VPN institucional podrá acarrear sanciones disciplinarias, contractuales o legales, según las normativas vigentes.

Las demás especificaciones están definidas en el documento *GTI10-POL01 Política de Acceso a la Red Privada Virtual de la CGN*.

7.17. Política de Administración de Usuarios y Contraseñas

Esta política se encarga de documentar los lineamientos de gestión de usuarios, perfiles y contraseñas.

a. Toda cuenta debe estar vinculada a un usuario único, debidamente identificado y autorizado.
b. La creación y activación de cuentas se realizará previa solicitud formal realizada por el jefe inmediato y utilizando el formato de gestión de usuarios.
c. Las cuentas inactivas por más de 60 días serán deshabilitadas automáticamente.
d. Los accesos a los servicios de TI y servicios tecnológicos serán asignados bajo el principio de mínimo privilegio y según funciones específicas.
e. Cualquier elevación de privilegios debe estar justificada y autorizada por el jefe inmediato y hacer uso del formato de gestión de usuarios.
f. Al finalizar el vínculo laboral o contractual, los accesos de los usuarios se revocan diligenciando el formato GAD22-FOR03 Paz y salvo por retiro de la entidad.
g. Está prohibido compartir contraseñas o anotarlas en lugares visibles.

h. Las cuentas en el controlador de dominio se bloquearán tras 3 intentos fallidos de autenticación consecutivos.
i. Se mantienen los logs de auditoría a algunos servicios específicos de TI en el marco de registrar actividades realizadas a ciertos procesos específicos y se conservarán al menos por 6 meses.

Las demás especificaciones están definidas en el documento *GTI02-POL01* Política de Administración de Usuarios y Contraseñas.

7.18. 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. Toda la información de la CGN (pública, pública clasificada y pública reservada) debe estar protegida para evitar que personas no autorizadas la consulten, divulguen o modifiquen sin consentimiento a terceras partes (colaboradores y entidades externas).
b. Si la información no está clasificada como pública, esta no podrá ser proporcionada a ninguna entidad externa sin un acuerdo de confidencialidad.
c. 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 a los correos institucionales seguridadinformatica@contaduria.gov.co y mesadeservicio@contaduria.gov.co, con el objeto de realizar un control efectivo de posibles daños y tomar las acciones necesarias.
d. Ningún servidor público o colaborador que tenga alguna relación laboral o contractual con la CGN 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 donde se incluyan aspectos técnicos de infraestructura.
e. 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 pueda identificar la clasificación de la información de la entidad en cualquier momento (consultar *GTI12-INS01- Instructivo para la gestión de activos de la información*).

f. Toda la documentación relacionada en el formato *GTI12-FOR01 Inventario de activos de información* debe estar etiquetada indicando el nivel de sensibilidad con base en la clasificación de pública clasificada y pública reservada.
g. Todo el personal de planta, contratistas, entes estratégicos u otros deben firmar el acuerdo de confidencialidad de la CGN.
h. El acceso a información confidencial estará limitado a usuarios que lo requieran para el cumplimiento de sus funciones y cuenten con autorización formal por parte del jefe inmediato.
i. Se realizarán campañas y capacitaciones periódicas sobre el manejo adecuado de información confidencial.

7.19. Política de Criptografía y Llaves Criptográficas

El proceso de Gestión TICs de la CGN 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. Para ello, se siguen los siguientes lineamientos:

a. Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que se ha comprometido su confidencialidad. En el caso de los certificados SSL, la periodicidad es de uno (1) o dos (2) años, de acuerdo con la disponibilidad presupuestal.
b. La administración de llaves criptográficas y certificados digitales está a cargo del proceso de Gestión TICs; sin embargo, la administración de tokens bancarios está a cargo del proceso de Gestión Administrativa. Dichos tokens generan una llave dinámica de un solo uso OTP (One Time Password autenticación con multifactor (MFA)) para el acceso a las diferentes plataformas.
c. Los servidores públicos o colaboradores a quienes les sean asignados tokens físicos son responsables de su custodia cuando no los estén utilizando.
d. Se utilizarán únicamente algoritmos criptográficos reconocidos como seguros.

e. Los certificados digitales deben ser emitidos por autoridades certificadoras confiables.
f. El uso de certificados para firma electrónica o autenticación deberá cumplir con la legislación vigente.

7.20. Política de Acceso Físico

La administración del edificio cuenta con procedimientos para el ingreso, entrega de carga y tránsito por zonas comunes, al ser parte de la propiedad horizontal de este edificio. La CGN deberá acatar e incluir estos procedimientos dentro de su funcionamiento, de acuerdo con lo establecido en el documento *Manual de Seguridad Física de la Administración del Edificio Elemento*, destacando los siguientes aspectos:

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.

7.21. Política de Áreas Seguras

Con el propósito de prevenir el acceso no autorizado a las instalaciones de la entidad, la CGN cuenta con los siguientes lineamientos, los cuales se describen en el flujograma de seguridad física y del entorno del documento *GTI-PRC10 Procedimiento de seguridad de la información*.

a. El ingreso a las áreas de la CGN se debe hacer a través de una puerta de acceso delimitada por la zona de recepción.
b. El acceso de visitantes al Centro de Datos se debe realizar con acompañamiento de un colaborador del proceso de Gestión TICs, y se debe registrar tanto el ingreso como la salida en el formato *GTI02-FOR01 Bitácora Plataforma Tecnológica*, con el fin de dejar evidencia.
c. 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 aloja.

d. Las áreas críticas como el centro de datos debe contar con cámaras de seguridad (CCTV) registrando actividad las 24 horas.

e. La CGN cuenta con un plan de emergencias, con el fin de brindar protección contra amenazas externas.

f. El Centro de Datos cuenta con un sistema de detección de incendios que le permite reaccionar de manera automática ante la presencia de fuego o humo.

g. El centro de datos debe ubicarse en zonas controladas, sin exposición directa a fuentes de riesgo (agua, fuego, polvo, etc.). y debe disponer de UPS, sistemas redundantes y protección eléctrica.

7.22. Política de Ubicación y Protección de los Equipos

a. En el centro de datos de la CGN se deben ubicar los equipos de infraestructura tecnológica como servidores, almacenamientos, seguridad perimetral, switches, router, entre otros que permiten la operación de los servicios de TI y Tecnológicos.

b. El Centro de Datos de la CGN debe contar 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), aire acondicionado y corriente regulada.

c. Se debe hacer seguimiento a las condiciones (temperatura, humedad, voltaje, y apertura y cierre de puertas) que pueden llegar a afectar los equipos en operación 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 o bandejas de distribución).

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 registrarse en el formato *GTI02- FOR04 Gestión de cambios TI*.

h. El centro de datos y la red LAN de la entidad deberá contar con un sistema de alimentación no interrumpida redundante (UPS) que asegura un tiempo mínimo necesario de funcionamiento de los equipos tecnológicos ante una falla en el suministro de energía. Adicionalmente, el edificio cuenta con una planta eléctrica.

i. 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.

j. El proceso de Gestión TICs debe coordinar las labores de mantenimiento correctivo, preventivo y evolutivo de los equipos de infraestructura tecnológica del centro de datos y de oficina como equipos de cómputo e impresoras, las cuales se realizan a través de los responsables de la infraestructura tecnológica y con el apoyo de los proveedores que tienen contrato vigente. Adicionalmente, se debe realizar seguimiento a los planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.

k. Todos los dispositivos de la plataforma tecnológica deben mantener su software actualizado con los parches de seguridad más recientes

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

m. Todos los equipos del centro de datos y en general equipos tecnológicos de oficina deben estar conectados a fuentes de energía estabilizadas y de protección con sistemas UPS.

n. Debe implementarse protección contra sobrecargas, descargas y picos de voltaje.

o. El cableado debe estar organizado, identificado y canalizado, evitando obstrucciones y puntos de desconexión accidentales.

p. El acceso a equipos del centro de datos será exclusivo del personal del GIT de apoyo informático o autorizado y registrado mediante mecanismos de control físico o lógico.

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

r. Los responsables de cada proceso deben aplicar las normas mínimas de seguridad física en las áreas en donde estén instalados equipos de cómputo.

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

Cualquier equipo portátil debe ser debidamente asegurado si se va a dejar desatendido. Es necesario guardarlo bajo llave.

7.23. Política para el Uso de Medios Removibles, Borrado Seguro y Disposición de Medios

Define las reglas y lineamientos para la protección de datos en diferentes medios de almacenamiento removible, así como el manejo de borrado seguro y disposición de medios, con el fin de evitar la divulgación no autorizada, modificación, borrado y destrucción de activos de información e interrupción de las actividades del negocio.

- Los medios removibles de propiedad de la entidad deben mantenerse bajo custodia del GIT de apoyo informático, evitando extravíos o acceso no autorizado.
- Serán inactivados los puertos USB de los equipos de cómputo de la CGN y solo previa solicitud de autorización al GIT de apoyo informático por parte del coordinador respectivo, será activado.
- Previo a la reutilización o eliminación de un medio extraíble o disco interno debe aplicarse un método de eliminación segura como la sobreescritura con herramientas especializadas, desmagnetización (para discos magnéticos), destrucción física.

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

7.24. Política de Pantalla Despejada y Escritorio Limpio

a. Todos los equipos de cómputo y servidores de los centros de datos la CGN deberán ser 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 equipo de cómputo en el momento en que se retiren de la misma, de forma tal que solo se pueda desbloquear con la contraseña de usuario.

c. El usuario antes de retirarse del equipo de cómputo debe finalizar la sesión de los servicios de TI que esté utilizando y bloquear manualmente el equipo con el comando Windows + L, en teletrabajo con Ctrl+Alt-Fin.

d. Los equipos de cómputo ubicados en el puesto de trabajo deben apagarse completamente al final de la jornada de trabajo, con la excepción para los casos en los que la entidad le haya asignado un equipo de cómputo remoto, para lo cual este equipo remoto deberá permanecer encendido, bloqueado, finalizada la sesión en los servicios de TI y con la pantalla apagada.

e. Los archivos que contengan información sensible deberán ser almacenados en los servicios de TI dispuestos por la entidad como carpetas compartidas y almacenamiento de nube, no se deben guardar en el área de escritorio de la pantalla del computador.

f. La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que los servidores públicos o colaboradores ejerzan sus funciones o cumplan sus obligaciones contractuales, según el caso.

g. Los documentos electrónicos que generan los servidores públicos o colaboradores en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, deben guardarse en los servicios de almacenamiento dispuestos por la entidad como la carpeta compartida de red o en la nube (OneDrive).

h. Los servidores públicos o colaboradores 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.

i. Al imprimir información reservada o pública clasificada, los documentos deberán ser retirados de forma inmediata de las impresoras y en caso de

no utilizarse deben destruirse para evitar divulgación no autorizada de la información.

j. Los servidores públicos o colaboradores que tengan dentro de sus funciones la atención al público deberán guardar los documentos físicos 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.

k. En la infraestructura tecnológica ubicada en los centros de datos luego de su uso siempre se debe cerrar sesión.

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

m. En las áreas visibles al público o a visitantes como salas de espera, recepción y reuniones, se debe extremar la precaución para que no haya documentos o pantallas con información reservada o pública clasificada a la vista.

7.25. Política de Control de Virus o software malicioso

a. La CGN es responsable de suministrar un sistema de antivirus, el cual debe estar instalado, activo y actualizado periódicamente en cada equipo de cómputo, 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 sospeche que han sido comprometidos por virus o software malicioso deben ser desconectados de la red de forma inmediata. El usuario debe solicitar apoyo al soporte técnico del GIT de Apoyo Informático e informar a los correos seguridadinformatica@contaduria.gov.co y mesadeservicio@contaduria.gov.co.

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 CGN.

e. El sistema de protección antivirus debe incluir escaneo en tiempo real, escaneo programado; y prevenir, detectar, contener y erradicar software malicioso.

7.26. Política de Respaldo y restauración de Datos

a. Las copias de respaldo de la infraestructura misional se ejecutan diariamente mediante una estrategia combinada de respaldos incrementales y selectivos totales, entendiéndose selectivos como la elección de determinados file systems a los cuales se les hace un backup total e incremental con la herramienta de la CGN.

b. Cada servidor cuenta con una planificación específica orientada a proteger datos críticos, incluyendo bases de datos, archivos de las aplicaciones desplegadas y logs. Los respaldos de configuración del sistema se programan principalmente durante los fines de semana, siguiendo también una estrategia incremental y total selectiva, adaptada a las características y necesidades de cada ambiente.

c. Para el custodio externo de los medios de respaldo de la plataforma misional, éste debe contar con los controles de seguridad necesarios para su almacenamiento y gestión relacionada con la entrega o retiro de estos al responsable designado por el GIT de Apoyo Informático.

d. Las copias de respaldo para la infraestructura de gestión se realizan de manera total con periodicidades diarias, semanales, mensuales, bimensuales, trimestrales, semestrales y anuales. Se deja evidencia en un archivo de control de backup.

e. Las copias de respaldo para los usuarios de la CGN se realizan de manera total al término de su contrato o relación laboral con la Entidad.

f. Las copias de respaldo de la configuración de la infraestructura de red y seguridad perimetral se realizan semanalmente.

g. Las copias de respaldo de las configuraciones de la plataforma, de los servicios de TI y tecnológicos se realizarán mensualmente

h. El periodo de retención de las copias de respaldo de gestión está sujeto a el periodo de las copias de seguridad. Ejemplo: Una copia diaria tendría una retención de hasta (2) días a razón del esquema abuelo, padre e hijo.

i. El periodo de retención de las copias de respaldo de los usuarios de la CGN es de hasta (2) años después de terminado su contrato o relación laboral con la Entidad.

Para la restauración de datos

Las restauraciones de datos para la infraestructura misional se realizan de manera semestral. Este proceso consiste en tomar una copia de respaldo de un servicio de TI misional y restaurarlo en la plataforma de contingencia, con el objetivo de validar la integridad de los datos y garantizar la continuidad operativa ante posibles contingencias.

Las restauraciones de los servidores en la infraestructura de gestión se realizan de manera trimestral, tomando de manera aleatoria un servicio de TI de gestión y restaurarlo en la plataforma de contingencia garantizando que el sistema operativo inicie de manera correcta y así mismo validar la integridad de los datos y garantizar la continuidad de la operación de servicio.

Las restauraciones de datos para los usuarios de la CGN se realizan bajo la solicitud del usuario a través de la mesa de servicios.

Las restauraciones de las configuraciones de la infraestructura de red y seguridad perimetral se realizan en el evento que se dé una actualización de firmware o que alguna configuración realizada lo requiera.

Las restauraciones de las configuraciones de la plataforma tecnológica se realizan en el evento que se dé una actualización o que alguna configuración realizada lo requiera.

Las demás especificaciones están definidas en el documento *GTI03-POL01 Política de Copias de Respaldo*.

7.27. Política de Sincronización de Relojes de los sistemas

Con el fin de obtener un control apropiado para la correlación 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 CGN deben estar sincronizados automáticamente con la hora legal colombiana mediante el protocolo NTP (Network Time Protocol). Esta responsabilidad corresponde al GIT de Apoyo Informático.

Los servidores NTP que utilice la CGN para sincronizar toda la infraestructura tecnológica automáticamente cada periodo de tiempo, deben ser reconocidos y seguros.

7.28. Política de Gestión de la Vulnerabilidad Técnica

a. El proceso de Gestión TICs es responsable de verificar de manera periódica la información publicada por parte de los fabricantes y foros de seguridad en relación 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 vulnerabilidades detectadas deben ser clasificadas según su criticidad en baja, media, alta y crítica y establecer el plan de remediación en el tiempo estableciendo la prioridad y determinando cuáles son alcanzables de acuerdo con los recursos técnicos, humanos y económicos asignados al proceso Gestión TICs; así como establecer medidas de mitigación en el caso de no ser posible la corrección de la vulnerabilidad.

d. Luego de ser aplicada la remediación se deben realizar pruebas para validar su efectividad y asegurar que no se comprometa la operación.

e. Las acciones correctivas que requieran ser aplicadas en la plataforma tecnológica y servicios de TI, derivadas de la identificación de vulnerabilidades técnicas, son responsabilidad del proceso de Gestión TICs y se registrará en el formato *GTI02-FOR04 Administración de Cambios a TI*.

7.29. 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 de información.

b. Se firmarán acuerdos de confidencialidad con los servidores públicos, colaboradores o terceros que por diferentes razones requieran conocer o intercambiar información clasificada y reservada. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de información de cada una de las partes y se deberán firmar antes del acceso o uso de dicha información.

c. Los servidores públicos o colaboradores deben seguir las indicaciones del procedimiento *GTI-PRC12 - Gestión de activos de la información*, 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. La CGN establece los mecanismos criptográficos para garantizar la confidencialidad, integridad y disponibilidad de la información durante su transferencia.

f. Se debe transferir información únicamente a receptores autorizados, a quienes se les informará el tipo de información objeto de transferencia y su deber de adoptar medidas orientadas a conservar la información dependiendo de su tipo.

g. Solo se permitirá transferir información institucional a través de canales autorizados como: correo electrónico institucional con cifrado habilitado, transferencia vía SFTP o FTPS, servicios de almacenamiento en la nube con control de acceso, red privada virtual VPN para accesos remotos. No se permite el intercambio de información a través de medios no autorizados por la entidad como correos personales, plataformas de mensajería instantánea no institucionales, almacenamiento en la nube sin validación de seguridad.

h. Los emisores deben validar la identidad de los destinatarios previamente al envío de la información clasificada como pública reservada, con el fin de reducir la posibilidad de envío a destinatarios no deseados.

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

j. Antes de transferir cualquier información, esta se debe revisar con un software antivirus y/o 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 *GTI12-INS01 Instructivo para la gestión de activos de la información*.

l. Cuando la información sea entregada en medios físicos (CD, USB, documentos impresos), estos deben estar protegidos físicamente y, si es necesario, cifrados, ser entregados directamente a personal autorizado, registrando la fecha y firma de entrega

7.30. Política para Desarrollo y Mantenimiento de Software

a. Establece los términos y condiciones para el desarrollo y mantenimiento de software en la CGN, teniendo en cuenta las partes que intervienen de los procesos, así como la parte funcional y técnica.

b. Esta política abarca desde el estudio de viabilidad funcional de la solicitud, ya sea una incidencia o un nuevo requerimiento, hasta la liberación de versión a producción. Las especificaciones están definidas en el documento *GTI07-POL01 Política de Desarrollo y Mantenimiento de Software*.

c. El software debe desarrollarse siguiendo un enfoque basado en buenas prácticas de codificación segura (ej. OWASP). Se deben implementar validaciones de entrada, manejo seguro de errores, gestión de sesiones, autenticación y control de acceso.

d. Se deben mantener separados los ambientes de desarrollo, pruebas y producción, evitando el uso de datos reales en ambientes no productivos. Cada entorno tendrá accesos restringidos y definidos por roles.

e. Todo el código fuente de las aplicaciones y sistemas de información debe gestionarse mediante un sistema de control de versiones y documentar el historial de cambios.

f. Los cambios al software que se definan deben ser solicitados, aprobados, probados y registrados en el formato de Gestión de cambios de TI GTI02-FOR04

g. Se deben evaluar periódicamente las dependencias y bibliotecas externas del software para identificar vulnerabilidades conocidas (CVE). Las fallas detectadas deben corregirse conforme a su criticidad.

7.31. Políticas para Proveedores de Servicios

Define los lineamientos de seguridad para los proveedores que, en el desarrollo de sus funciones, puedan tener acceso a sistemas de información o recursos en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la CGN.

Los accesos físicos o lógicos otorgados a proveedores serán temporales, mínimos y autorizados formalmente, los mismos deben ser revocados al terminar el servicio.

Para iniciar el servicio deben firmar el acta de inicio del contrato, acuerdo de confidencialidad, dar a conocer por parte de la CGN las políticas de seguridad de la información; en la reunión de inicio el proveedor debe reconocer los acuerdos de servicio, obligaciones, tiempos de ejecución y formas de pago establecidas en el contrato.

Las demás especificaciones están definidas en el documento *GTI10-POL02 Política de seguridad para proveedores de servicios*.

7.32. Política de Gestión de eventos e incidentes de Seguridad de la Información

a. La entidad controla el reporte y evaluación de los eventos o incidentes de seguridad de la información, tales como afectación de confidencialidad, integridad y disponibilidad de la información mediante el manejo de dichos incidentes de acuerdo con el flujograma de Gestión de Incidentes de Seguridad de la Información del *GTI-PRC10 Procedimiento de seguridad de la información*.

b. Se debe 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.

- Todo el personal de la CGN debe estar vigilante con respecto a los eventos, incidentes o debilidades de seguridad (pérdida de información o dispositivos, acceso no autorizado, infección por virus, suplantación de identidad, divulgación de información clasificada, caídas o interrupciones graves de servicios de TI). Por lo tanto, si se detectan estos eventos o incidentes se deben reportar de forma inmediata al encargado de gestionarlos a los correos seguridadinformatica@contaduria.gov.co y mesadeservicio@contaduria.gov.co.

d. Se deben notificar a los correos seguridadinformatica@contaduria.gov.co y mesadeservicio@contaduria.gov.co. situaciones como personas ajenas a la CGN en oficinas y centros de cómputo, correos maliciosos, sospechas de equipos infectados, reinicio de los equipos de cómputo, mala utilización de recursos, uso ilegal del software, mal uso de información institucional, alteración de información, entre otros.

e. Los incidentes se clasifican según su impacto en menor, moderado o mayor, evaluando su afectación en los procesos, activos, usuarios y reputación. El equipo del Git de apoyo informático debe contener la propagación, identificar el origen, restaurar los servicios afectados y documentar el caso.

7.33. Política para uso de servicios en la nube

La CGN establece los requisitos y procedimientos necesarios para garantizar la seguridad de la información al utilizar servicios de nube pública y privada, incluyendo la protección de datos, la gestión de accesos y la continuidad del servicio.

1. Los servicios en nube son responsabilidad del GIT de Apoyo Informático, teniendo en cuenta:

a. Acuerdos de niveles de servicio de 99.5% como mínimo.

b. Gestionar el acceso de los usuarios en la nube.

d. Los canales de conexión a la nube deben ser seguros, usar protocolos que permitan la encriptación de las comunicaciones entre el navegador y el servidor web

e. Se debe realizar una autenticación segura.

f. Se debe contar con contraseñas robustas

g. Gestionar la capacidad y disponibilidad del servicio en la nube.

2. Para el uso de servicios en la nube, se deben identificar y valorar los riesgos asociados a dicho servicio.

3. Se deben establecer mecanismos de registro para las actividades realizadas sobre el almacenamiento en la nube.

4. Se deben establecer los medios de acceso, los dispositivos que tienen acceso, las ubicaciones desde las cuales se puede acceder a los servicios en la nube.

5. Las estrategias del respaldo de la información alojada en la nube, se basan en las plataformas de los proveedores del servicio (Google y Microsoft).

7. Los servidores públicos, contratistas, proveedores o terceros que tengan acceso a la información institucional, son responsables del otorgamiento de accesos y permisos a las carpetas que compartan desde la nube a otras personas.

8. Es responsabilidad de los servidores públicos y/o contratistas, la descarga y uso adecuado de la información de la nube en equipos personales.

7.34. Política de Continuidad de Negocio

La Contaduría General de la Nación, como entidad rectora responsable de regular la contabilidad general de la nación, 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 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 CGN establece como prioridad la preservación de la vida e integridad de sus servidores públicos, colaboradores y demás partes interesadas.

Las especificaciones del plan están definidas en el documento *GTI-PLN01 Plan de continuidad del negocio de TI* y contempla de manera general que, 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 con los lineamientos establecidos por la entidad.

7.35. Política de Contingencia de los Servicios Tecnológicos

El GIT de Apoyo Informático de la CGN identificará y anticipará, de manera permanente, la pérdida de las capacidades de infraestructura tecnológica de procesamiento, almacenamiento, seguridad informática y redes de comunicaciones que impacten los procesos críticos del negocio, de apoyo y estratégicos esenciales ante eventos que afecten la disponibilidad, para lo cual se actualizarán las guías asociadas a los servicios seleccionados de acuerdo a su criticidad de recuperación de los componentes de la plataforma tecnológica.

Para el plan de contingencia se establece un programa de pruebas, el cual deberá ejecutarse de manera que simule las condiciones de un evento y no se afecte la operación, ni los ANS acordados con las partes interesadas. Las pruebas deben ser planeadas, documentadas y deberán incluir las recomendaciones, planes de acción y lecciones aprendidas respectivas.

Las especificaciones están definidas en el documento *GTI-PLN02 Plan de Contingencia Tecnológica*.

7.36. Política de Protección de los Derechos de Autor

a. Es política de la CGN el cumplimiento de todas las obligaciones legales, adquiriendo el material patentado de la empresa propietaria o duplicándolo bajo expresa autorización de esta.
b. La CGN garantiza el respeto de los derechos de autor y el uso legal de obras protegidas por propiedad intelectual en todas las actividades desarrolladas, promoviendo el cumplimiento legal y ético.
c. La CGN adquiere software legal o utiliza software que tenga licencia válida, y solo el personal del GIT de Apoyo Informático en cumplimiento de sus funciones u obligaciones, está autorizado para instalarlo en las estaciones de trabajo de la entidad.
d. Solo está permitido utilizar software previamente autorizado, adquirido legalmente o que cuente con licencia válida. Se prohíbe la instalación de

software pirata, crackeado o de procedencia dudosa.

e. El personal de la CGN que utilice imágenes, videos, música, textos o artículos protegidos por derechos de autor debe validar que este contenido cuente con licencia expresa o estar bajo régimen de uso libre (Creative Commons, dominio público, etc.). Se prohíbe utilizar, copiar o reutilizar contenidos sin autorización o sin atribución cuando aplique.
f. 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 o colaboradores que trabajan para la CGN 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 transgresión de derechos en cierto software, bajo la Ley de Derechos de Autor, constituye una infracción legal.
g. Se debe cumplir a cabalidad con todas las leyes, normas, decretos, sentencias y demás normativas que sean aplicables.
h. Las obras desarrolladas por los funcionarios o contratistas en cumplimiento de sus funciones u obligaciones (documentos, aplicaciones, presentaciones, procedimientos, etc.) son propiedad de la entidad.

7.37. Política de Conflictos Legales

Las políticas de seguridad de la información de la CGN 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, debe reportarlo de forma inmediata al Oficial de Seguridad y Privacidad de la Información y al correo institucional seguridadinformatica@contaduria.gov.co y mesadeservicio@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 PI24-POL01 política de privacidad y protección de datos personales de la CGN.

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, artículos, softwares, licencias y códigos 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 con lo establecido en la Ley de Delitos Informáticos 1273 del 2009 y demás aplicables.

7.38. Política de Monitoreo y Evaluación del Cumplimiento

a. El personal de GIT de Apoyo Informático en cumplimiento de sus funciones u obligaciones tiene la responsabilidad de monitorear los equipos de cómputo portátiles con el fin de identificar lo que pueda ser considerado como software ilegal o aplicaciones que afecten la seguridad de la información.

b. La CGN 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 o colaboradores 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 y archivos en colas de impresión.

c. Debido a que los sistemas de cómputo y comunicaciones suministrados por la CGN se emplean únicamente para propósitos de la entidad, los servidores públicos o colaboradores no deben tener expectativas de privacidad asociadas con 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 de la plataforma colaborativa o el Coordinador del GIT de Apoyo Informático no facilitará a otra persona el contenido de ningún archivo de correo electrónico del personal activo con contrato, sin obtener el permiso del usuario o, en su defecto, del jefe inmediato (aplica solamente para cuando la persona tiene una relación laboral vigente con la entidad), cuando exista un motivo razonable para hacerlo. Dichos motivos pueden incluir, sin limitarse a ello, mantener la integridad del sistema (como la eliminación de virus), cumplir obligaciones legales

(como citaciones judiciales) y efectuar ciertas funciones de administración del sistema (como remitir los mensajes con direcciones erróneas).

f. No obstante, la CGN puede obtener acceso a la información de los servidores públicos o colaboradores en caso de que se requiera dicha información para investigaciones o en caso de emergencia. Por ejemplo, si el servidor público, colaborador o tercera parte está ausente durante un periodo prolongado de tiempo debido a enfermedad u otro motivo (previa autorización escrita del jefe inmediato), o no tiene vínculo laboral vigente en el tiempo, se podrá tener acceso a la información para suplir necesidades del servicio y para las investigaciones pertinentes.

g. La CGN 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 información de la entidad.

8. Bibliografía

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). Política General de Seguridad de la Información. https://gobiernodigital.mintic.gov.co/692/articles-272947_recurso_1.zip

Organización Internacional de Normalización y Comisión Electrotécnica Internacional. *ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información.*

Elaboró: Martha Zornosa Guerra / Diana Murillo Calderón
Revisó: Anuar Vargas Calderón y EAOS
Aprobó: Freddy Castaño Pineda y EAOS

Revisado por: Anuar Vargas Calderón	**Aprobado por:** Claudia Hernández Diaz
LÍDER DEL PROCESO DE GESTIÓN TIC´S	**REPRESENTANTE DE LA DIRECCIÓN LÍDER DEL PROCESO DE PLANEACIÓN INTEGRAL**