SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/11/2024	GTI-POL00	01	**1** de **31**

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

NOVIEMBRE DE 2024

SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/11/2024	GTI-POL00	01	**2** de **31**

CONTROL DE CAMBIOS

VERSIÓN	SECCIÓN	TIPO	FECHA (DD/MM/ AAAA)	AUTOR	OBSERVACIONES
1.0	Todas	Actualización	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 solamente 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

SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/11/2024	GTI-POL00	01	**3** de **31**

CONTENIDO

SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	N/A		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/11/2024	GTI-POL00	01	**5** de **31**

1. INTRODUCCIÓN

Este documento describe 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 se constituyen como 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 y es responsabilidad de todos los servidores públicos y colaboradores de la CGN conocer y cumplir las siguientes políticas con el fin de usar los recursos tecnológicos de manera responsable y segura.

Todo evento o incidente de seguridad deberá ser reportado a los correos seguridadinformatica@contaduria.gov.co y mesadeservicio@contaduria.gov.co.

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

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

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

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

6.1. 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.

6.2. Política de Dispositivos Móviles

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. Durante los viajes, los equipos (y medios) no se deben dejar desatendidos en lugares públicos. Los computadores portátiles se deben llevar como equipaje de mano.

c. 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.

d. 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).

e. Los equipos de cómputo de la CGN, 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.

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 servidor público o colaborador que lo tenga asignado.

g. Las estaciones de trabajo y equipos portátiles que son propiedad de la CGN cuentan con software licenciado y protección contra código malicioso.

h. El servidor público o colaborador que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato será responsable de:

- 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.

6.3. Política de Teletrabajo y Trabajo Remoto

La CGN establece los lineamientos de teletrabajo en la Resolución 171 de 2023, por la cual se adopta la modalidad de teletrabajo, 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.

d. Establecer comunicación segura mediante el uso de canales VPN establecidos por el GIT de Apoyo Informático.

e. 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.

f. Está prohibido el envío de archivos con información institucional por medios no oficiales, tales como Dropbox, WeTransfer, correos de dominio gratuito, etc.

g. La sesión establecida con la CGN no debe ser utilizada por una persona diferente al servidor público o colaborador autorizado.

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

i. Está terminantemente prohibido establecer conectividad con un equipo de cómputo diferente al asignado o autorizado para teletrabajo o trabajo remoto.

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

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

6.4. Política para el Talento Humano

Esta política define los lineamientos para la selección y vinculación del personal, además de las consideraciones para la desvinculación del personal de planta. Así mismo, define los lineamientos para la contratación directa de servicios profesionales.

a. Planta: las especificaciones están definidas en los documentos *GTH-PRC19 Selección y vinculación de personal de planta* y *GTH-PCR20 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*.

c. El personal de la CGN se compromete mediante el documento *MAN01-FOR31 Acuerdo de confidencialidad y aceptación de las políticas de la seguridad de la información* a mantener la confidencialidad de manera indefinida en caso de retiro.

6.5. 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 que se tengan en uso 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.

6.6. Política de Procesos Disciplinarios

Los procesos disciplinarios en la CGN se llevan a cabo de acuerdo con la Ley 1952 de 2019 - Principios y normas rectoras de la ley disciplinaria, modificada por la Ley 2094 de 2021, por parte de Secretaría General.

6.7. 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 entregados 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 pueden almacenar, instalar o utilizar juegos en los equipos de cómputo de la CGN.

d. Únicamente los servidores públicos y/o colaboradores de soporte autorizados por la CGN, 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 CGN. 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. A menos que sean específicamente autorizados por el Coordinador del GIT de Apoyo Informático, los servidores públicos o colaboradores de la CGN 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 CGN 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 CGN.

h. La CGN se reserva el derecho de examinar toda la información almacenada o transmitida por sus sistemas de cómputo y de comunicación, y debe informar a los servidores públicos o colaboradores 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 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".

6.8. 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.

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 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.

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; esta práctica puede derivar en un proceso disciplinario.

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 deberá cambiar la contraseña inmediatamente y reportar a los correos institucionales seguridadinformatica@contaduria.gov.co y mesadeservicio@contaduria.gov.co, adjuntando la evidencia.

n. 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 dispuestas para este componente.

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

6.9. 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, 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 discriminatorio, racista, o material potencialmente ofensivo, o relacionado con situaciones de menosprecio o acoso implícito.

6.10. 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 PI-PRC28 - Gestión de activos de información.

b. Asignación de activos: La asignación de equipo de cómputo se realiza de acuerdo con las obligaciones del servidor público o colaborador, y los requerimientos solicitados por el líder del proceso.

c. Uso aceptable de los activos:

1. La información (física y digital), los sistemas de información, servicios y equipos (por ejemplo: 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 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* (PI-PRC28), el *Instructivo de gestión de activos de información* (PI28-INS01) y el formato *Inventario de activos de información* (PI28-FOR01).
3. Los equipos informáticos que son adquiridos por la entidad deberán etiquetarse con número de inventario en el área de almacén antes de que sean asignados.
4. En caso de que el servidor público o colaborador deba hacer uso de equipos ajenos a la CGN, estos deberán cumplir con la legalidad del software instalado, antivirus licenciado y actualizado, y solo podrá conectarse a la red de la CGN una vez esté autorizado por la Coordinación del GIT de Apoyo Informático.
5. 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*.

6.11. Política de Clasificación de Información

La CGN 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 CGN, 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 o colaboradores deben familiarizarse con las definiciones de estas categorías y cumplir con las medidas de protección establecidas para ellas.

6.12. Política de Control de Acceso

a. 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 y gestionado por el GIT de Apoyo Informático.

b. Todos los sistemas conectados a la red de la CGN deben solicitar el usuario de acceso a la red y contraseña, la cual tendrá un máximo de tres (3) intentos fallidos. Se debe asegurar que la 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.

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 computadora multiusuario, servidores o recursos de sistemas y aplicaciones en producción.

d. Los sistemas no deben permitir sesiones simultáneas con el mismo usuario de acceso a la red desde diferentes equipos de cómputo.

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

f. Las novedades (vacaciones, incapacidades, 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 cuales tengan acceso.

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

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

i. Se deben revisar dos veces al año los derechos de acceso de los usuarios a los sistemas y a los servicios de información para mantener un control eficaz.

j. 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-FOR09* **-** *Solicitud creación de cuentas institucional y/o*

VPN.

k. 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.

l. Se deberá utilizar la conexión de acceso remoto solo para acceder a servicios (aplicativos e infraestructura) exclusivos de la CGN.

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

n. 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 recursos a los cuales estuvo autorizado y se debe realizar también una devolución de activos.

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

6.13. Política de la Red Interna

La red interna de la CGN es un recurso vital que permite la comunicación, el intercambio de información y el acceso a recursos críticos 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. El acceso a la red interna está restringido a servidores públicos o colaboradores autorizados por la entidad. Se requiere autenticación para acceder a recursos y datos de la red.

b. El usuario de acceso a la red interna es personal e intransferible. Se prohíbe compartir las credenciales de acceso.

c. El uso de la red interna debe cumplir con las políticas y regulaciones establecidas en este documento.

d. Todos los dispositivos conectados a la red interna deben mantener su software actualizado con los parches de seguridad más recientes. Se promueve el uso del software antivirus debidamente licenciado y medidas de seguridad adicionales.

e. 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.

f. 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.

g. 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.

h. 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.

6.14. Política de Uso de la Red Inalámbrica Pública

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*.

6.15. 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 implicancias del mal uso.

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

6.16. Política de Administración de Usuarios y Contraseñas

Esta política se encarga de documentar los lineamientos de gestión de usuarios, perfiles y contraseñas. Las especificaciones están definidas en el documento *GTI02-POL01 Política de Administración de Usuarios y Contraseñas*.

6.17. 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 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 *PI28-INS01- Instructivo para la gestión de activos de la información*).

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

g. Toda la documentación relacionada en el formato *PI28-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.

6.18. 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 área solicitante. Dichos tokens generan una llave dinámica de un solo uso OTP 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.

6.19. 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.

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

e. 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.

6.21. Política de Ubicación y Protección de los Equipos

a. El Centro de Datos de la CGN 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 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 contemplar la revisión de las políticas de seguridad y el formato *GTI02- FOR04 Administración de cambios TI*.

h. La entidad cuenta con un sistema de alimentación no interrumpida redundante (UPS) que asegura el tiempo necesario de funcionamiento de los servidores, los cuales alojan los sistemas de información 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 coordina las labores de mantenimiento correctivo y preventivo, las cuales se realizan a través de los responsables de soporte, y cuando sea necesario será subcontratado dicho servicio. Adicionalmente, se realiza seguimiento a los planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.

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

l. Los equipos de cómputo o 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.

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

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

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

6.22. 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.

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

6.23. Política de Pantalla Despejada y Escritorio Limpio

a. Todos los equipos de 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 estación de trabajo 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 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.

d. 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.

e. Los archivos que contengan información personal sensible deberán ser almacenados en rutas que impidan el fácil acceso por parte de terceros, evitando, por ejemplo, guardarlos 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 la carpeta de almacenamiento en red dispuesta por la entidad.

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 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 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 los 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.

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.

6.24. Política de Control de Virus

a. La CGN 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 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.

6.25. Política de Respaldo de Datos

Define las políticas para realizar copias diarias, semanales, mensuales, anuales, en diferencial, diferencial incremental y total, de acuerdo con el tipo de copias de respaldo en el que se realice su almacenamiento. Las especificaciones están definidas en el documento *GTI03-POL01 Política de Copias de Respaldo*.

6.26. Política de Sincronización de Relojes

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 con la hora legal colombiana mediante el protocolo NTP. Esta responsabilidad corresponde al GIT de Apoyo Informático.

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

6.28. 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 *PI-PRC28 - 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. Se deben usar mecanismos criptográficos para garantizar la confidencialidad, integridad y disponibilidad de la información durante su transferencia, de acuerdo con su nivel de clasificación.

f. Se debe transferir información únicamente a receptores autorizados, quienes garanticen por escrito el tratamiento de la información que se les vaya a suministrar, por medio de acuerdos de 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 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 *PI28-INS01 Instructivo para la gestión de activos de la información*.

6.29. Política para Desarrollo y Mantenimiento de Software

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.

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*.

6.30. 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.

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

6.31. Política de Gestión de 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.

c. Todo el personal de la CGN debe estar vigilante con respecto a los eventos, incidentes o debilidades de seguridad (incluyendo fallas en el sistema, pérdida del servicio, datos del negocio incompleto o inadecuado, pérdida de la confidencialidad). Por lo tanto, si se detectan estos eventos, incidentes o debilidades de seguridad se deben reportar de forma inmediata al encargado de gestionar los eventos e incidentes de seguridad a los correos seguridadinformatica@contaduria.gov.co y mesadeservicio@contaduria.gov.co.

d. Se deben notificar 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 o enrutadores, mala utilización de recursos, uso ilegal del software, mal uso de información institucional, alteración de información, entre otros.

e. Toda violación de estas políticas se debe notificar inmediatamente al proceso de Gestión TICs y al líder del proceso, de modo que se pueda resolver debidamente el evento o incidente.

6.32. Política de Continuidad de Negocio

La UAE 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.

6.33. 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 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.

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*.

El GIT de Apoyo Informático identifica y anticipa permanentemente la pérdida de las capacidades de procesamiento de información que impacten los procesos críticos del negocio, para lo cual actualiza las guías de recuperación de los componentes de la plataforma tecnológica.

6.34. Política de 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. Todo el software operativo y aplicativo es propiedad de la CGN y solo el grupo de soporte técnico, con previa autorización del Coordinador del GIT de Apoyo Informático, está autorizado para instalarlo en las estaciones de trabajo de la entidad.
c. 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.

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

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

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

6.35. 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, lo debe reportar 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 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, 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.

6.36. Política de Monitoreo y Evaluación del Cumplimiento

a. El servidor público o colaborador asignado por el Coordinador del GIT de Apoyo Informático tiene, en primera instancia, 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 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 del correo o el Coordinador del GIT de Apoyo Informático no facilitará a otra persona 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 (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), 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.

7. 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 27001:2013, Information Technology. Security Techniques. Code of Practice for Information Security Controls*.

Organización Internacional de Normalización y Comisión Electrotécnica Internacional. *ISO/IEC 27002:2013, Information Technology. Security Techniques. Code of Practice for Information Security Controls.*

Organización Internacional de Normalización y Comisión Electrotécnica Internacional. *ISO/IEC 27001:2022, Information Technology. Security Techniques. Code of Practice for Information Security Controls*.

Revisado por: Jamir Mosquera Rubio	**Aprobado por:** Vilma Narváez Narváez
LÍDER DEL PROCESO DE GESTIÓN TIC´S	**REPRESENTANTE DE LA DIRECCIÓN LÍDER DEL PROCESO DE PLANEACIÓN INTEGRAL**