SEGURIDAD PARA PROVEEDORES DE SERVICIO			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
21/07/2026	GTI02-POL06	03	**1** de **5**

1. INTRODUCCIÓN

Los presentes documentos desarrollan, precisan y operacionalizan la política general de seguridad y privacidad de la información, así como las políticas de seguridad de la información y de seguridad digital, las cuales fueron adoptadas por el Comité Institucional de Gestión y Desempeño (CIGD) en sesión celebrada el 10 de octubre de 2025, conforme a lo consignado en el Acta No. 10 de 2025.

2. OBJETIVO:

Establecer los lineamientos de seguridad aplicables a los proveedores de servicios que, en el desarrollo de sus actividades, tengan acceso a sistemas, información o recursos tecnológicos de la Contaduría General de la Nación (CGN), con el propósito de proteger la confidencialidad, integridad y disponibilidad de la información institucional.

3. ALCANCE:

Esta política aplica a todos los proveedores, contratistas y terceros, que mantengan vínculos contractuales con la CGN y que, directa o indirectamente, accedan, procesen o custodien información o recursos tecnológicos de la entidad

4. DEFINICIONES

- **Activo crítico**: es un recurso (físico, digital, información o humano) cuya pérdida, interrupción o daño pueden afectar la operación, estabilidad y continuidad del negocio
- **Proveedor**: empresa que presta servicios bajo un contrato o convenio.
- **Servicios**: son funciones ejercidas por los proveedores hacia otras personas con lafinalidad de que estas cumplan con la satisfacción de recibirlos.
- **Contrato o convenio:** es un acuerdo de voluntades que se manifiesta en común entre dos omás personas (naturales o jurídicas).
- **VPN (Virtual Private Network o Red Privada Virtual)**: es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet, que permite el acceso remoto seguro a los recursos institucionales.
- **SLA (Service Level Agreement):** acuerdo formal de nivel de servicio que define compromisos de desempeño y seguridad.
- **Plan de Continuidad del Negocio (BCP):** estrategia y procedimientos definidos para garantizar la continuidad de las operaciones ante incidentes o desastres.

5. RESPONSABLES DE CUMPLIMIENTO:

- **Oficial de seguridad de la información:** supervisar y velar por el cumplimiento de esta política.
- **GIT Apoyo Informático:** apoyar el cumplimiento de esta política.
- **Proveedores:** responsable de cumplir a cabalidad con lo dispuesto en esta política y los compromisos contractuales asociados.

6. DESCRIPCIÓN DE POLÍTICAS

6.1. Ingreso a las instalaciones

a) Los proveedores deberán registrarse en el sistema de acceso institucional y en caso de llevar consigo un equipo portátil, este también deberá ser registrado.
b) Todo proveedor que ingrese a la CGN deberá portar el carnet de identificación de la empresa y el documento de visitante entregado en la recepción de forma visible durante el tiempo que dure su estadía en las instalaciones.
c) Por ningún motivo el personal que representa al proveedor podrá deambular por las instalaciones de la CGN en áreas no autorizadas.
d) Está prohibido el uso de equipos de registro (fotografía, video, audio, etc.) salvo autorización expresa por parte del GIT de Apoyo Informático.
e) Para los fines de semana, el ingreso de proveedores se hará con previa autorización del Coordinador del GIT de Apoyo Informático, mediante el formato establecido.

6.2. Confidencialidad de la Información.

a) Los proveedores, contratistas o terceros protegerán la información confidencial a la que tengan acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentre contenida esa información.
b) Todos los proveedores, contratistas o terceros deberán firmar un acuerdo de confidencialidad de la información con la CGN, el cual será de estricto cumplimiento.
c) Está prohibido intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados en virtud de la relación contractual o comercial.
d) Por ningún motivo el proveedor, contratistas o terceros intentará manipular o alterar los registros "log" de los sistemas de información.
e) El proveedor, contratistas o terceros no deberá introducir ningún tipo de malware, grayware, dispositivo lógico, dispositivo físico o cualquier otro tipo

de secuencia de órdenes que causen cualquier tipo de alteración o daño en los recursos informáticos.

f) El proveedor, contratistas o terceros deberá utilizar software de antivirus actualizado y contar con mecanismos de prevención de malware.

g) Los proveedores, contratistas o terceros con acceso a activos críticos de la CGN deberán contar con opciones de Continuidad del Negocio y estar preparados para enfrentar ataques contra la seguridad de la información que pueda afectar a la CGN.

h) Todos los proveedores, contratistas o terceros deben informar de los incidentes de seguridad física y de la información tan pronto se haya identificado su ocurrencia al correo electrónico seguridadinformatica@contaduria.gov.co o al correo mesadeservicio@contaduria.gov.co

6.3. **Uso de recursos**

a) Para los casos que se requiera, se creará al proveedor un correo electrónico con dominio de la CGN durante el tiempode ejecución del contrato.

b) Está prohibido el uso de los recursos dispuestos por la CGN para actividades no relacionadas con el propósito u objeto del servicio, o bien la extralimitación en su uso.

c) Los proveedores que tengan correo electrónico con dominio de la CGN no deberán crear, enviar o reenviar mensajes publicitarios o de tipo cadenas.

d) Para los proveedores que tengan correo electrónico con dominio de la CGN, su uso deberá limitarse a fines laborales, evitando mensajes de tipo cadena o publicidad

e) Está prohibido instalar en los equipos a los que tenga acceso el proveedor, cualquier software no autorizado, sin importar su modo de distribución.

6.4. **Gestión de accesos**

a) Para la creación de cuentas de usuario, buzón de correo y acceso a la Red Privada Virtual – VPN de la CGN de proveedores, se deberá gestionar el formato GTI10-FOR09 Gestión de cuentas de usuario, para los casos en que sea necesario.

b) Para cada sistema existe un conjunto de perfiles y privilegios que se atribuyen a los usuarios de acuerdo con el objeto del contrato.

c) El proveedor deberá cumplir las políticas de seguridad para el manejo de contraseñas establecido por la CGN.

d) Los privilegios de acceso a los sistemas son revocados de forma automática cuando finaliza el contrato con el proveedor.

6.5. Acceso a centro de cómputo

a) El acceso al centro de cómputo deberá ser controlado y supervisado por personal de la CGN.
b) El proveedor que ingrese al centro de cómputo deberá registrar su ingreso en el formato GTI02-FOR01 BITACORA PLATAFORMA TECNOLÓGICA.

6.6. Prestación de servicios desde la sede del proveedor.

a) La sede deberá contar con un sistema de control de acceso, que garantice la prevención ante robo, destrucción o interrupción del servicio.
b) La CGN se reserva el derecho de programar visitas de inspección de seguridad a la sede del proveedor.
c) El proveedor debe contar con sistemas de detección y prevención de incendios.

6.7. Prestación de servicios tecnológicos

a) Se definirán los acuerdos de niveles de servicios (SLA) en las especificaciones técnicas y en las cláusulas del contrato.
b) Dentro de los acuerdos de nivel de servicio (SLA) deberán incluir compromisos de seguridad y disponibilidad.
c) Todo cambio relacionado al ambiente de producción o pruebas en las plataformas instaladas, accedidas y manejadas local o remotamente, deben regirse al formato GTI02-FOR04 Gestión de cambios de TI de la CGN.
d) El proveedor deberá identificar y controlar los impactos ambientales que pudiesen presentarse durante la prestación del servicio.

6.8. Desarrollo de Software

a) Todo desarrollo que se realice para la CGN debe ser documentado y cumplir con los controles de seguridad definidos por la CGN.
b) El desarrollo de software no debe incluir ningún mecanismo que permita el acceso no autorizado al sistema, como identificaciones, contraseñas incrustadas, troyanos, puertas traseras u otros elementos similares.
c) El desarrollo de software deberá especificar cuales controles de seguridad aplica, incluyendo políticas de seguridad y procesos de desarrollo seguro.
d) Los desarrollos deberán incorporar prácticas de desarrollo seguro y validaciones técnicas antes de su entrega

7. Actualización de la política de seguridad para proveedores

La CGN se reserva el derecho a modificar esta política cuando sea necesario.

Los cambios realizados a esta política serán divulgados a todas las empresas proveedoras a las que les aplique, utilizando los medios pertinentes.

Es responsabilidad de cada proveedor garantizar la lectura y conocimiento de la política de Seguridad de la Información y la Política de Seguridad para Proveedores vigente.

Elaboró: Martha Zornosa Guerra
Revisó: Anuar Vargas Calderón e integrantes del EAOS
Aprobó: Freddy Castaño Pineda