

ACCESO A LA RED PRIVADA VIRTUAL DE LA CGN			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07//2026	GTI02-POL05	04	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, configuración y uso de la Red Privada Virtual (VPN) institucional, para garantizar un acceso remoto seguro a los servicios de TI y tecnológicos de la Contaduría General de la Nación (CGN), protegiendo la confidencialidad, integridad y disponibilidad de la información.

3. ALCANCE

Esta política aplica a todos los funcionarios, contratistas, colaboradores y proveedores que, a través de la autorización previamente otorgada por el GIT de Apoyo Informático, se acojan a los lineamientos establecidos en esta y que requieran conectarse remotamente a los sistemas, aplicaciones y demás servicios de TI de la CGN a través de VPN-SSL o VPN-IPSec.

4. DEFINICIONES

VPN: una VPN, o Red Privada Virtual, es una tecnología que crea una conexión segura y cifrada entre un dispositivo y una red privada a través de Internet. Esto protege la privacidad y la seguridad de los datos mientras se navega por la web o se accede a recursos en línea.

VPN SSL: (Secure Sockets Layer) es un tipo de VPN que utiliza el protocolo SSL/TLS para establecer conexiones seguras a través de Internet. Proporciona un acceso seguro a aplicaciones y recursos en línea, sin necesidad de instalar software adicional, mediante el uso de un navegador web y cifrado SSL para proteger la comunicación.

VPN IPSec: (Protocolo de Seguridad de Internet) es un tipo de VPN que utiliza IPSec para crear una conexión segura y cifrada entre dos dispositivos o redes. Es ampliamente utilizado para garantizar la confidencialidad e integridad de la comunicación a través de Internet, y se utiliza comúnmente en conexiones de red a red o cliente a red.

ACCESO A LA RED PRIVADA VIRTUAL DE LA CGN			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07//2026	GTI02-POL05	04	2 de 5

PreShared-Key: (PSK) o Clave Precompartida, es una contraseña compartida entre dos entidades que se utiliza para autenticar y cifrar la comunicación en una conexión segura, como una VPN. Ambas partes deben conocer esta clave antes de establecer la conexión para garantizar la seguridad de la comunicación.

Token de seguridad: dispositivo o aplicación que genera códigos temporales (OTP) para autenticación multifactor (MFA).

4. RESPONSABLES DE CUMPLIMIENTO

- **Oficial de Seguridad de la Información:** supervisar y velar por el cumplimiento de esta política.
- **GIT Apoyo Informático:** configurar, administrar, monitorear las conexiones VPN y los tokens de autenticación.
- **Usuarios autorizados y Proveedores:** cumplir los lineamientos establecidos, proteger sus credenciales y notificar cualquier incidente de seguridad.

5. RECOMENDACIONES DE USO DE LA VPN

La CGN se reservará el derecho de conexión por VPN y solo a través de la autorización que se haga al GIT de Apoyo Informático se establecerá el procedimiento para la creación y configuración de la VPN, y se entregará el instructivo donde se indican los pasos que debe seguir la persona autorizada para establecer dicha conexión, además de su responsabilidad en el correcto uso del servicio de acceso remoto.

El uso inapropiado de los recursos dispuestos para los usuarios expone a la entidad a riesgos innecesarios como virus informáticos, interrupción de las redes y sus sistemas y pérdida de información entre otros.

6. CONSIDERACIONES ADICIONALES

Solicitud y autorización:

Todas las personas que quieran acceder a los servicios de TI de la entidad a través de VPN deberán diligenciar totalmente el formato *GTI-10-FOR09 Gestión de cuentas de usuario*, solicitar dicho servicio a través de la herramienta de mesa de ayuda y cumplir con todas las disposiciones establecidas en el documento *Políticas de Seguridad de la Información y Seguridad Digital* de la entidad, además de la firma del acuerdo de confidencialidad de la información.

ACCESO A LA RED PRIVADA VIRTUAL DE LA CGN			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07//2026	GTI02-POL05	04	3 de 5

Para las conexiones de VPN IPSec que se establecen con otras entidades para acceder a los servicios del sistema de información CHIP deberán diligenciar el formato GTI10-FOR08 – Solicitud de VPN – IPSec con los parámetros que ahí se establecen.

Los accesos se habilitarán solo por el tiempo necesario y se revocarán automáticamente al finalizar el contrato o la relación laboral.

Autenticación y control de acceso:

Autenticación mediante token: todo acceso a la VPN requerirá **autenticación multifactor (MFA)** basada en:

- ✓ Credenciales de usuario institucional (usuario y contraseña).
- ✓ Token de seguridad personal (digital) que genera un código temporal de validación.

El token es personal e intransferible. Su pérdida o mal uso debe reportarse inmediatamente al GIT de Apoyo Informático.

El administrador de red definirá los perfiles y políticas de acceso para cada usuario o servicio, restringiendo el acceso únicamente a los recursos autorizados, garantizado que no se tendrá acceso a otros servicios distintos a los autorizados

Solo se permitirá una sola conexión establecida, es decir, no se permitirá multiplicación paralela de túneles VPN.

Requisitos técnicos:

Los equipos que establezcan conexión VPN deberán contar con antivirus, sistema operativo vigentes y actualizados y bloqueo con contraseña segura, con el fin de garantizar la seguridad de la conexión.

Todas las personas conectadas a la VPN serán automáticamente desconectadas de la sesión una vez hayan transcurridos 10 minutos de inactividad. Se establecerá dentro de la política de acceso la restricción de denegación de servicios y no se permitirán procedimientos similares para mantener la sesión abierta. Una vez la sesión sea desconectada, la persona deberá iniciar sesión (*login*) nuevamente.

ACCESO A LA RED PRIVADA VIRTUAL DE LA CGN			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07//2026	GTI02-POL05	04	4 de 5

La disponibilidad del servicio de conexión por VPN es de 7 a 5 pm, el cual está definido en el catálogo de servicios de TI, así como su ANS correspondiente.

VPN-IPSec para interconexión con otras entidades:

Las conexiones de VPN IPSec son permanentes y se garantiza su seguridad a través de la PreShared-Key compartida entre las dos entidades las cuales deben ser seguras (longitud y complejidad de caracteres). La entidad remota deberá informar el tiempo de uso de la misma conexión o si la CGN verifica que la conexión se encuentra "No establecida" procederá a informar de la misma a la entidad remota a través del correo electrónico descrito en el formato GTI10-FOR08 – Solicitud de VPN – IPSec.

Los parámetros de encriptación y autenticación deben ser correspondidos entre las dos entidades como mecanismo de seguridad de la conexión.

Las conexiones serán permanentes, salvo notificación de la entidad remota o finalización de convenio.

Condiciones de uso y responsabilidades de usuario:

Es responsabilidad de la persona que tiene privilegios de acceso remoto por VPN velar por que la cuenta de acceso no sea utilizada por otra persona ni permitir que los accesos queden expuestos sobre los equipos desde donde se establece la conexión.

El usuario deberá garantizar que su cuenta de VPN no se utilizada por terceros.

Se prohíbe compartir credenciales, tokens o claves precompartidas

Todo incidente o intento de acceso no autorizado deberá reportarse inmediatamente a seguridadinformatica@contaduria.gov.co o mesadeservicio@contaduria.gov.co

Como se entiende que la conexión por VPN establece una extensión de la red de datos de la CGN, los computadores institucionales o personales están sujetos a las mismas normas y reglamentos que se aplican a los equipos dentro de las dependencias de la entidad.

ACCESO A LA RED PRIVADA VIRTUAL DE LA CGN			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07//2026	GTI02-POL05	04	5 de 5

Monitoreo:

El GIT de Apoyo Informático conservará por un periodo de tiempo registros de auditoría (logs) de todas las conexiones VPN (usuario, IP, hora, duración, actividad). Los registros serán revisados periódicamente para detectar comportamientos anómalos o intentos de intrusión.

Trabajo en casa:

Cuando se presente un evento donde se deba realizar trabajo en casa de manera indefinida, se notificará al servidor público, colaborador o proveedor a través de la cuenta de correo institucional las instrucciones para conectarse vía VPN. Si es necesario, el personal técnico asistirá al usuario en el procesos de configurar la VPN.

Elaboró: Martha Zornosa Guerra / Diana Murillo Calderón

Revisó: Anuar Vargas Calderón e integrantes del EAOS

Aprobó: Freddy Castaño Pineda