1. INTRODUCCIÓN

La política de uso de la Red Privada Virtual tiene como objetivo principal, ofrecer a los funcionarios, contratistas y colaboradores una guía sobre las características y requerimientos mínimos que deben ser cumplidos para el uso correcto del servicio de VPN institucional y cualquier mecanismo de acceso remoto a los servicios que provea la Contaduría General de la Nación, como también las implicancias del mal uso.
Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios expone a la entidad a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, perdida de información, etc.

2. ALCANCE

Teniendo en cuenta el alcance de la Política de Seguridad Informática de la entidad es importante definir que el uso apropiado que se haga de la Red Privada Virtual, tanto para las conexiones por VPN SSL y VPN IPSec aplicará no solo a los funcionarios de planta sino a todos los proveedores, contratistas y colaboradores que, a través de la autorización previamente otorgada, se acojan a los lineamientos establecidos en la Política de Seguridad Informática y a la misma Política de acceso por VPN.

3. RECOMENDACIONES DE USO DE LA VPN

La Contaduría General de la Nación se reservará el derecho de conexión por VPN y solo a través de la autorización que se haga al Administrador de la Red de datos de la entidad se establecerá el procedimiento para la creación y configuración de la VPN y entregar el documento donde se indican los pasos que debe seguir la persona autorizada para establecer dicha conexión y su responsabilidad en el correcto uso del servicio de acceso remoto.

4. CONSIDERACIONES ADICIONALES

1. 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.

2. La persona con privilegios de acceso por VPN deberá acercarse al GIT de Informática para que pueda ingresar su contraseña de acceso a la conexión y asegurándose de mantenerla en secreto.

> *Nota: 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, personal técnico asistirá al usuario en el proceso de configurar el VPN.*

3. El Administrador de la Red de Datos y del Firewall creará un perfil y política de acceso hacia el recurso o servicio informático al cual la persona autorizada tendrá acceso una vez se

establezca la conexión por VPN, garantizando que no tendrá acceso a otros recursos o servicios distintos a los autorizados.

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

5. Para garantizar la seguridad de la conexión es importante que las conexiones que se realicen por VPN o por otro medio de conexión remota hacia los computadores o servidores de la entidad estén protegidos por Antivirus validando que este se encuentra actualizado hasta la última base de datos de definiciones por el proveedor del antivirus. Es importante también que los equipos de las personas autorizadas se encuentren protegidas por esta herramienta con el fin de hacer más segura la conexión remota.

6. 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 loguearse nuevamente aplicando una nueva sesión.

7. El horario de conexión por VPN definido en el firewall o concentrador se establece en una relación de 7x24, garantizando el servicio de conexión permanentemente.

8. Todas las personas que quieran acceder a los recursos informáticos de la entidad a través de la VPN deberán diligenciar totalmente el formato GTI-10-FOR04 Solicitud de cuentas de usuario institucional – VPN, solicitar dicho servicio a través de la herramienta de mesa de ayuda y cumplir con todas las disposiciones establecidas en la Política y Manual de Seguridad de la Información de la entidad, además de la firma del acuerdo de confidencialidad de la información.

9. Como se entiende que la conexión por VPN establece una extensión de la red de datos de la Contaduría General de la Nación, 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.

10. Las conexiones por VPN o acceso remoto se autorizarán de acuerdo con el tiempo que se establezca en la solicitud ya sea por la duración del contrato o del servicio que se vaya a prestar.

11. 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.

12. 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 de 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.

13. Los parámetros de Encriptación y Autenticación deben ser correspondido entre las dos entidades como mecanismo de seguridad de la conexión.