POLÍTICA DE RED PRIVADA VIRTUAL (VPN)

Visión general

El acceso remoto a equipos, servidores y servicios informáticos es cada vez más frecuente, principalmente por la modalidad de teletrabajo y la necesidad de administrar servicios que requieren una disponibilidad 24/7. Por este motivo es mandatorio definir lineamientos tecnológicos que permitan establecer conexiones privadas y seguras entre los equipos remotos y las redes de Gobierno.

Objetivo

El propósito de esta política es establecer un estándar para las conexiones de Red Privada Virtual (VPN) entre los equipos remotos y las redes de Gobierno, a través de internet.

Alcance

El alcance de esta política incluye a toda persona física (personal de planta, contratados, subcontratados, etc.) que realice tareas que requieran la conexión a las redes de Gobierno a través de internet por una Red Privada Virtual (VPN).

Política de Red Privada Virtual (VPN)

Es responsabilidad de los empleados, contratistas, proveedores y agentes que tengan privilegios de acceso remoto a las redes de Gobierno, usar una conexión habilitada por VPN.

Los empleados y terceros autorizados pueden utilizar el servicio de VPN que es administrado por el mismo usuario. Esto significa que el usuario es responsable de seleccionar un proveedor de internet (ISP), e instalar cualquier software requerido.

Procedimientos de conexión

1. Es responsabilidad de los empleados con privilegios de conexión VPN asegurar que usuarios no autorizados tengan acceso a las redes privadas de Gobierno.

2. El uso de la VPN para usuarios finales debe ser controlado exclusivamente a través de cuentas contenidas y gestionadas a través del servicio de Directorio de Gobierno, nominadas en el dominio sanjuan.gob o en sus subdominios.

3. Los usuarios estándar sólo tendrán acceso remoto a su PC de escritorio dentro de la organización.

4. La administración de servidores y servicios tecnológicos se realizará a través del servicio de Escritorio Remoto (RDS).

5. Las cuentas que requieran privilegios especiales deberán ser otorgados o quitados a través de Políticas de Grupo (GPO) y Unidades Organizativas (OU) dentro del servicio de directorio.

6. Sólo se otorgarán privilegios especiales a usuarios cuya tarea no pueda ser realizada mediante el servicio de Escritorio Remoto (RDS). Las solicitudes de privilegios especiales deberán ser correctamente justificadas y autorizadas por un superior. La Dirección de Ciberseguridad evaluará cada caso y tendrá la facultad de aceptar o rechazar cada solicitud.

7. Existirán 2 (dos) cuentas locales en el concentrador VPN con privilegios de administración para casos excepcionales:

- admin_DCS: Administrador local para la Dirección de Ciberseguridad. El/la Director/a será responsable de esta cuenta.
- admin_DRyCD: Administrador local para la Dirección de Redes y Centro de Datos. El/la Director/a será responsable de esta cuenta.

8. Cuando la conexión VPN sea establecida, todo el tráfico relacionado a las redes de Gobierno pasarán por el túnel VPN. El tráfico con destino a internet seguirá el camino por defecto de su proveedor de internet.

9. Todo equipo conectado a las redes de Gobierno a través del servicio de VPN deben usar software licenciado con las actualizaciones más recientes y disponer de software antivirus con las últimas firmas de seguridad.

10. Los usuarios VPN se desconectarán automáticamente después de 30 minutos de inactividad. En caso de superar ese tiempo, el usuario deberá restablecer la conexión.

11. El acceso remoto a equipos de Gobierno, solo se podrá realizar mediante clientes VPN aprobados por Gobierno. Queda prohibido el uso de herramientas como AnyDesk, TeamViewer, otros.

12. Al utilizar el servicio de VPN con equipos personales, los usuarios aceptan y entienden que sus máquinas son una extensión de facto de la red de Gobierno y por lo tanto están sujetas a las mismas normas y reglamentos que se aplican a los equipos de la organización. Los equipos deben cumplir con las Políticas de Seguridad de la Información de Gobierno.

Cumplimiento de la política

Medición de cumplimiento

La Dirección de Ciberseguridad verificará el cumplimiento de esta política a través de varios métodos, que incluyen, entre otros, recorridos periódicos, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas y comentarios al propietario de la política.

Incumplimiento

Un empleado que se descubra que ha violado esta política puede estar sujeto a medidas disciplinarias.