

PROTOCOLO |||
PROVINCIAL DE CIBERSEGURIDAD

**Estándar de TI:
Estándar de Acceso Remoto**

05
CAPÍTULO



Estándar de TI: Estándar de Acceso Remoto

1.0 Propósito y Beneficios

El propósito de este estándar es establecer métodos autorizados para acceder de forma remota a recursos y servicios de forma segura.

Los principales problemas de seguridad con el acceso remoto incluyen la falta de controles de seguridad físicos, el uso de redes no seguras, la conexión de dispositivos infectados a redes internas, la disponibilidad de recursos internos para hosts externos, posibles daños a los recursos y el acceso no autorizado a la información.

2.0 Alcance

Esta norma se aplica a la autenticación de cuentas que acceden a sistemas de tecnología de la información con el fin de realizar actividades administrativas gubernamentales de forma electrónica remota.

3.0 Declaración de información

Se permite el acceso remoto cuando existe una necesidad administrativa clara y documentada. Se puede permitir el acceso desde dispositivos emitidos por la entidad o de propiedad personal, a discreción del MPEyM y de acuerdo con los estándares a continuación. Dicho acceso debe limitarse únicamente a aquellos sistemas necesarios para las funciones necesarias.

3.1 MÉTODOS APROBADOS DE ACCESO REMOTO

Los métodos aprobados de acceso remoto a los sistemas se enumeran en orden de preferencia.

- a. **Portales** – un servidor que ofrece acceso a una o más aplicaciones a través de una única interfaz centralizada que proporciona autenticación (por ejemplo, portal basado en web, interfaz de escritorio virtual (VDI)).
- b. **Acceso directo a la aplicación** – acceder a un sistema directamente con los métodos de seguridad proporcionados por la misma aplicación (por ejemplo, correo web, https).

- c. **Control remoto del sistema** – controlar un sistema a distancia desde una ubicación distinta de la red interna del Gobierno de Jujuy.
- d. **Túnel** – un canal de comunicación seguro a través del cual se puede transmitir información entre redes (por ejemplo, Red Privada Virtual (VPN)).

3.2 CONTROLES REQUERIDOS

- a. Cualquier método de acceso remoto debe utilizar un sistema de autenticación administrado centralmente para la administración y el acceso de los usuarios.
- b. Los dispositivos y el software utilizados para el acceso remoto deben ser aprobados después de la revisión por parte del Oficial de Seguridad de la Información/responsable de seguridad designado. Se pueden proporcionar aprobaciones generales basadas en esta revisión.
- c. El token de autenticación utilizado para el acceso remoto debe cumplir con los requisitos del nivel de garantía adecuado.
- d. Las sesiones de acceso remoto deben requerir una nueva autenticación después de 30 minutos de inactividad.
- e. Las sesiones de acceso remoto no deben durar más de 08 horas.
- f. La entidad debe monitorear conexiones remotas no autorizadas y otras actividades anómalas y tomar las medidas apropiadas de respuesta a incidentes según lo establecido en Estándar de respuesta a incidentes cibernéticos.
- g. Controles específicos de túneles:
 - (a) Se permiten túneles divididos. (Split Tunneling)
 - (b) Se requieren controles de red que regulen el acceso remoto del *endpoint*; entre dispositivos remotos y las redes involucradas.
 - (c) Cuando un dispositivo de acceso remoto tenga acceso a otros dispositivos conectados en red en la red interna laboral, el dispositivo remoto debe autenticarse de manera que la configuración del dispositivo cumpla con las políticas aplicables.

4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias apropiadas, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación

de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

5.0 Definiciones de términos clave

Término	Definición
Endpoint	Es un dispositivo cualquiera que se encuentre conectado a una red informática.
Split Tunneling	Un túnel dividido en una VPN, permite enrutar parte del tráfico (por ejemplo, de las aplicaciones laborales) mientras que el tráfico a internet se enruta por el acceso a internet local de la red.

6.0 Historial de revisiones

Fecha	Descripción de Cambio	Crítico
13-06-2024	Draft final del documento	Alejandro Castro Pablo Zalazar
14-06-2024	Agregados en 6.0 Términos Clave, arreglos menores en documento.	Alejandro Castro

7.0 Documentos relacionados

Publicación especial 800-46 del Instituto Nacional de Estándares y Tecnología (NIST), Guía para el teletrabajo empresarial y la seguridad del acceso remoto

Publicación especial del NIST 800-113, Guía de VPN SSL

Publicación especial del NIST 800-114, Guía del usuario para proteger dispositivos externos para teletrabajo y acceso remoto