**Política de Herramientas de Acceso Remoto**

**Exención de responsabilidad:** Esta política fue creada por o para el Instituto SANS para la comunidad de Internet. Toda o parte de esta política se puede utilizar libremente para su organización. No se requiere aprobación previa. Si desea contribuir con una nueva política o una versión actualizada de esta política, envíe un correo electrónico a [policy-resources@sans.org](mailto:policy-resources@sans.org).

**Último estado de actualización:** *actualizado junio 2014*

# Visión general

El software de escritorio remoto, también conocido como herramientas de acceso remoto, proporciona una forma para que los usuarios de computadoras y el personal de soporte compartan pantallas, accedan a sistemas de computadoras de trabajo desde el hogar y viceversa. Entre los ejemplos de dicho software se incluyen LogMeIn, GoToMyPC, VNC (Virtual Network Computing) y Windows Remote Desktop (RDP). Si bien estas herramientas pueden ahorrar mucho tiempo y dinero al eliminar viajes y permitir la colaboración, también brindan una puerta trasera a la red de <Nombre de la empresa> que puede usarse para el robo, el acceso no autorizado o la destrucción de activos. Como resultado, solo las herramientas de acceso remoto aprobadas, monitoreadas y adecuadamente controladas pueden usarse en los sistemas informáticos de <Nombre de la empresa>.

# Propósito

Esta política define los requisitos para las herramientas de acceso remoto utilizadas en <Nombre de la empresa>

# Alcance

# Esta política se aplica a todos los accesos remotos donde cualquiera de los extremos de la comunicación termina en un activo de computadora de <Nombre de la empresa>

# Política

Todas las herramientas de acceso remoto utilizadas para comunicarse entre los activos de <Nombre de la empresa> y otros sistemas deben cumplir con los siguientes requisitos de políticas.

4.1 Herramientas de Acceso Remoto

<Nombre de la empresa> proporciona mecanismos para colaborar entre usuarios internos, con socios externos y desde sistemas que no son <Nombre de la compañía>. La lista de software aprobada se puede obtener en <enlace-a-lista-de-software-de-acceso-remoto-aprobada>. Debido a que la configuración adecuada es importante para el uso seguro de estas herramientas, se proporcionan procedimientos de configuración obligatorios para cada una de las herramientas aprobadas.

La lista de software aprobada puede cambiar en cualquier momento, pero se utilizarán los siguientes requisitos para seleccionar los productos aprobados:

1. Todas las herramientas o sistemas de acceso remoto que permiten la comunicación a los recursos de <Nombre de la empresa> desde Internet o sistemas de socios externos deben requerir la autenticación de múltiples factores. Los ejemplos incluyen tokens de autenticación y tarjetas inteligentes que requieren un PIN o contraseña adicional.
2. La fuente de la base de datos de autenticación debe ser Active Directory o LDAP, y el protocolo de autenticación debe incluir un protocolo de desafío-respuesta que no sea susceptible de ataques de repetición. La herramienta de acceso remoto debe autenticar mutuamente ambos extremos de la sesión.
3. Las herramientas de acceso remoto deben admitir el proxy de capa de la aplicación <Nombre de la empresa> en lugar de conexiones directas a través de los servidores de seguridad perimetrales (Firewalls).
4. Las herramientas de acceso remoto deben admitir un cifrado sólido de extremo a extremo de los canales de comunicación de acceso remoto tal como se especifica en la política de protocolos de cifrado de red <Nombre de la empresa>.
5. Todos los sistemas de seguridad, prevención de pérdida de datos y otros sistemas de seguridad de <Nombre de la empresa> no deben ser desactivados, interferidos o burlados de ninguna manera.

Todas las herramientas de acceso remoto deben adquirirse a través del proceso de adquisición estándar de <Nombre de la empresa>, y el grupo de tecnología de la información debe aprobar la compra.

# Cumplimiento normativo

* 1. Medición de cumplimiento

El equipo de INFOSEC verificará el cumplimiento de esta política a través de varios métodos, incluyendo, pero no limitado a, Walk-thrus periódico, monitoreo de video, informes de herramientas de negocios, auditorías internas y externas, y retroalimentación a la propietario de la póliza.

# Excepciones

Cualquier excepción a la póliza debe ser aprobada por el INFOSEC TEAM de antemano.

# Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, incluyendo la terminación del empleo.

# Normas, políticas y procesos relacionados

Ninguno.

# Definiciones y términos

La siguiente definición y términos se pueden encontrar en el Glosario de SANS que se encuentra en:

https://www.sans.org/security-resources/glossary-of-terms/

* Aplicación de capa de Proxy

# Historial de revisión

|  |  |  |
| --- | --- | --- |
| **Fecha de cambio** | **Responsable** | **Resumen de cambio** |
| Junio 2014 | El equipo de políticas SANS | Actualizado y convertido a nuevo formato. |
|  |  |  |