# Trey Research Corporation

Redes privadas virtuales: Información general técnica de Fabrikam, Inc.

15 de diciembre de 2023

**Las redes privadas virtuales (VPN)** son una solución de seguridad de red popular que puede ayudar a cifrar el tráfico de red. [Las VPN actúan como un túnel seguro y cifran el tráfico de Internet, lo que dificulta que terceros realicen un seguimiento de las actividades y roben datos](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1.](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)

## Ventajas de implementar VPN:

* Las VPN ofrecen una capa de privacidad y seguridad al cifrar el tráfico de Internet. Esto dificulta que terceros supervisen las actividades y roben datos.
* Las VPN pueden ayudar a evitar pirateos al utilizar la Wi-Fi pública en un aeropuerto o en la biblioteca. Esto se debe a que las VPN funcionan como un túnel seguro y cifran el tráfico de Internet.
* [Las VPN pueden impedir que su proveedor de servicios de Internet sepa qué sitios ha visitado porque el tráfico que llega a y desde su equipo viaja a través de los servidores de la VPN o los VPN de los servidores paga para usar](https://www.bing.com/aclk?ld=e83gkJ29qbmUu8cYkNgVfaCjVUCUx3vCyorXNIwmWui8A8rISGT4ATMfXuQu_8nGJifMsVNZrD0_vVyNtSvYRynbmDYfM2jUvwoREzv_CIrOKnWn2gIEyYOWegOAxJPNIFOUp5hBSGQU35pxcSs4Qxqzw59vf63cS8Oh_e_94A9QZD8MND&u=aHR0cHMlM2ElMmYlMmZ3d3cudnBubWVudG9yLmNvbSUyZmluLXVzYS1iZXN0LXZwbiUzZmtleXdvcmQlM2R2cG4lMjUyMHJhbmtpbmclMjZnZW8lM2QxMTA3MzUlMjZkZXZpY2UlM2QlMjZ1dG1fc291cmNlJTNkYmluZyUyNmFkaWQlM2Q3NjIxMDA1Nzk0MzY4MCUyNm1zY2xraWQlM2Q3NTEzMDFiNzM2MTQxZTY2ZTBiZDY0MTA0MzJlYjBkYw&rlid=751301b736141e66e0bd6410432eb0dc) [1.](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)
* [Las VPN pueden omitir las restricciones geográficas en el contenido 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/) enmascarando la dirección IP y cifrando la conexión a Internet. Cuando se conecta a un servidor VPN, el tráfico de Internet se enruta a través del servidor VPN, que le asigna una nueva dirección IP. [Esto hace que aparezca como si estuviera accediendo a Internet desde una ubicación diferente, lo que le permite omitir las restricciones geográficas en el contenido.](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## Inconvenientes de implementar VPN:

* Las velocidades de conexión pueden ser más lentas que el ISP. [Esto se debe a que las VPN agregan una capa adicional de cifrado y enrutamiento al tráfico de Internet 2.](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)
* El uso de VPN está prohibido en algunos países autoritarios. [En algunos países, las VPN están prohibidas o fuertemente reguladas](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/) [2.](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)
* El uso de VPN gratuitas corre riesgos de exposición a anuncios, malware y fugas. [Las VPN gratuitas pueden vender datos de usuario a anunciantes de terceros o insertar anuncios en páginas](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/) [web 2.](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)

## Detalles específicos de la instalación:

* [Una VPN establece un túnel cifrado entre el sistema que ejecuta el cliente VPN y un servidor VPN que, a continuación, proxies el tráfico a través del túnel al resto de la red](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [empresarial 4.](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/) Se incluyen los siguientes pasos:
  1. Se instala un cliente VPN en el dispositivo del usuario, que cifra todo el tráfico entre el dispositivo y el servidor VPN.
  2. El servidor VPN descifra el tráfico y lo reenvía al destino previsto.
  3. El servidor de destino responde a la solicitud al enviar el tráfico de vuelta al servidor VPN.
  4. El servidor VPN cifra el tráfico y lo envía de vuelta al cliente VPN.
  5. [El cliente VPN descifra el tráfico y lo envía al dispositivo](https://www.bing.com/aclk?ld=e8OcZUYHFbvxJgBgmEWpxgCzVUCUz-UOb13n9w7mOCOGgLkPnDhd3Uh-ipDjPE6Hpo4QBuX2o2EUlY6g5-dRpoq53O3haHMQ8RcFRpVU95xD1yO9RVjEOu3gsgBNFb6xmA-Gvbq-gT8RFWo2P6R0BeJBd5LyAIvbSKlU_DPbqAqdr2ubUB&u=aHR0cHMlM2ElMmYlMmZ3d3cub3BlcmEuY29tJTJmZmVhdHVyZXMlMmZmcmVlLXZwbiUzZnV0bV9zb3VyY2UlM2RiaW5nJTI2dXRtX21lZGl1bSUzZHBhJTI2dXRtX2NhbXBhaWduJTNkVVMlMjUyMC0lMjUyMFBlcmZvcm1hbmNlJTI1MjBNYXglMjUyMC0lMjUyMEVOJTI2dXRtX2NvbnRlbnQlM2QlN2Jhc3NldEdyb3VwSWQlN2QlMjZtc2Nsa2lkJTNkZDVhYzJiMDEzNDM2MWVkNDRmNGE0ZWE2NDA1MDk5MjIlMjZ1dG1fdGVybSUzZHd3dy5vcGVyYS5jb20&rlid=d5ac2b0134361ed44f4a4ea640509922) [del usuario 1.](https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html)
* Para instalar y configurar un servidor VPN, siga estos pasos:
  1. Crear un perfil VPN en su equipo.
  2. Hacer clic en iniciar y luego en Configuración para abrir el menú de configuración.
  3. En el menú de configuración, hacer clic en Red e Internet y luego en VPN.
  4. Seleccione Agregar una conexión VPN.
  5. En la ventana Agregar una conexión VPN, debe realizar algunas tareas.
  6. Guarde los cambios realizados.

## Riesgos y mitigaciones:

* Los atacantes saben que el trabajo remoto es un vector de amenaza desde hace tiempo. El entorno de trabajo remoto es especialmente atractivo para los atacantes por diversos motivos. En primer lugar, el entorno de la red doméstica no se administra de forma profesional. Esto significa que muchos más sistemas en redes domésticas no reciben revisiones con regularidad y muchos de ellos están anticuados respecto a la mitigación de vulnerabilidades. Para persistir en una red empresarial, el atacante que ha vulnerado el sistema debe evitar la detección y resistir la corrección. Aquí también, la red doméstica ayuda al atacante. La detección de amenazas está casi ausente y la corrección es fortuita, como cuando se reinstala o retira un equipo porque funciona lento. Para proteger el entorno de trabajo remoto, es fundamental ampliar todavía más las hipótesis de confianza cero. [No es solo la red que debe asumirse hostil, sino todo lo que no está bajo el control](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [de la empresa 4.](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/)
* [Actualice las VPN, los dispositivos de infraestructura de red y los dispositivos que se usan para realizar tareas remotas en entornos de trabajo con las últimas revisiones de software y configuraciones](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [de seguridad 6.](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a)

## Procedimientos recomendados para la implementación:

Los procedimientos recomendados para implementar VPN en una red corporativa incluyen los siguientes:

* [Seleccione una VPN basada en estándares que use estándares aceptados, como Internet Key Exchange/Internet Protocol Security (IKE/IPSec), que generalmente son menos arriesgados y más seguros que las VPN de capa de sockets seguros/Seguridad de la capa de transporte (SSL/TLS) que usan código personalizado para enviar tráfico a través de TLS 12.](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)
* Utilizar una VPN con criptografía sólida. Validar que los algoritmos de cifrado, algoritmos de autenticación y los protocolos que utiliza una VPN sean sólidos y validados para FIP. [Configure todas las VPN para usar la autenticación multifactor (MFA) y reemplace la autenticación basada en contraseña por la autenticación de cliente a través de certificados digitales (almacenados en tarjetas inteligentes) siempre que sea posible 12.](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)
* Administrar las vulnerabilidades de software. La explotación de las vulnerabilidades de VPN es un vector de ataque común para los ciberdelincuentes. Seleccionar un proveedor de VPN con un historial sólido de revisiones de vulnerabilidades y solicitar una lista de materiales de software (SBOM) para validar que el código de terceros esté actualizado y sea seguro. Además, buscar un producto que pueda realizar la validación de su código al ejecutarse para detectar posibles intrusiones. [Después de implementar una VPN, compruebe periódicamente las actualizaciones](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [de software 12](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/) y aplique rápidamente.
* Prepararse para las sobrecargas de uso. [El personal de seguridad de TI debe probar las limitaciones de VPN en preparación para el uso](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/) [masivo 2.](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/)
* Evitar las VPN gratis. [El uso de VPN gratuitas corre riesgos de exposición a anuncios, malware y fugas 3.](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/)