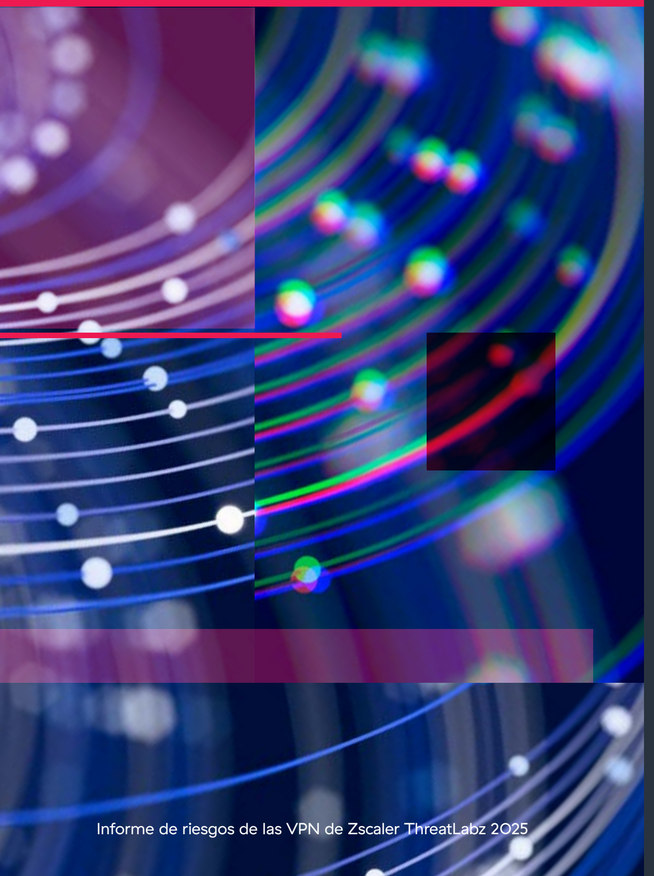
zscaler™ | Cybersecurity INSIDERS

# Zscaler Informe de riesgos de las VPN de ThreatLabz 2025



©2025 Zscaler, Inc. Todos los derechos reservados.

# Tabla de contenido




**Resumen ejecutivo** 3

**Hallazgos clave** 4

**Riesgos de las VPN: ¿Por qué el 81 % de las organizaciones adoptarán Zero Trust para 2026?** 5

**Preocupaciones sobre la seguridad de las VPN** 6

- La obsolescencia de las VPN: riesgos de seguridad y frustraciones de los usuarios 6
- Ransomware y VPN: una tormenta perfecta de riesgos 7
- VPN y movimiento lateral: aumento del radio de alcance de violaciones 8

**CVE de VPN de 2020 a 2025: una ola creciente de vulnerabilidades de alta gravedad** 9

- Tendencias clave: Tipos de impacto de las CVE 10
- Tendencias clave: vulnerabilidades críticas de VPN 11

**Preocupaciones sobre la seguridad de las VPN (cont.)** 13

- Los desafíos de aplicar la segmentación 13
- Las VPN aumentan los riesgos de ciberseguridad en las fusiones y adquisiciones 14
- Acceso a VPN de terceros: Una puerta trasera para los atacantes 15

**Desafíos y brechas de las medidas de protección heredadas** 16

- Las herramientas tradicionales dejan al descubierto las aplicaciones privadas 16
- Implementación de NAC en entornos VPN: una salvaguarda limitada 17

**Experiencia de usuarios de VPN y problemas de gestión** 18

- El problema del rendimiento de las VPN: frustración de los usuarios y sobrecarga de TI 18
- Gestión de VPN: sobrecarga de los equipos informáticos y exposición de vulnerabilidades 19
- La dura carga de la gestión de VPN 20
- Controles de acceso a VPN demasiado amplios: Una brecha de seguridad crítica 21
- Sustitución de VPN: Un cambio hacia el acceso seguro 22

**Adopción de Zero Trust** 23

- Zero Trust reemplaza a las VPN a gran escala 23
- Prioridades Zero Trust: el trabajo remoto impulsa la adopción 24
- Principales ventajas de sustituir las VPN por Zero Trust 25

**Predicciones de riesgo de VPN para 2025** 26

**Mejores prácticas para el acceso seguro** 28

- Reducir los riesgos de las VPN y fortalecer la seguridad Zero Trust 28

**Cómo Zscaler transforma el acceso seguro** 30

- Principales ventajas de Zscaler Private Access (ZPA) 31

**Metodología y Demografía** 33

**Acerca de** 34




©2025 Zscaler, Inc. Todos los derechos reservados.

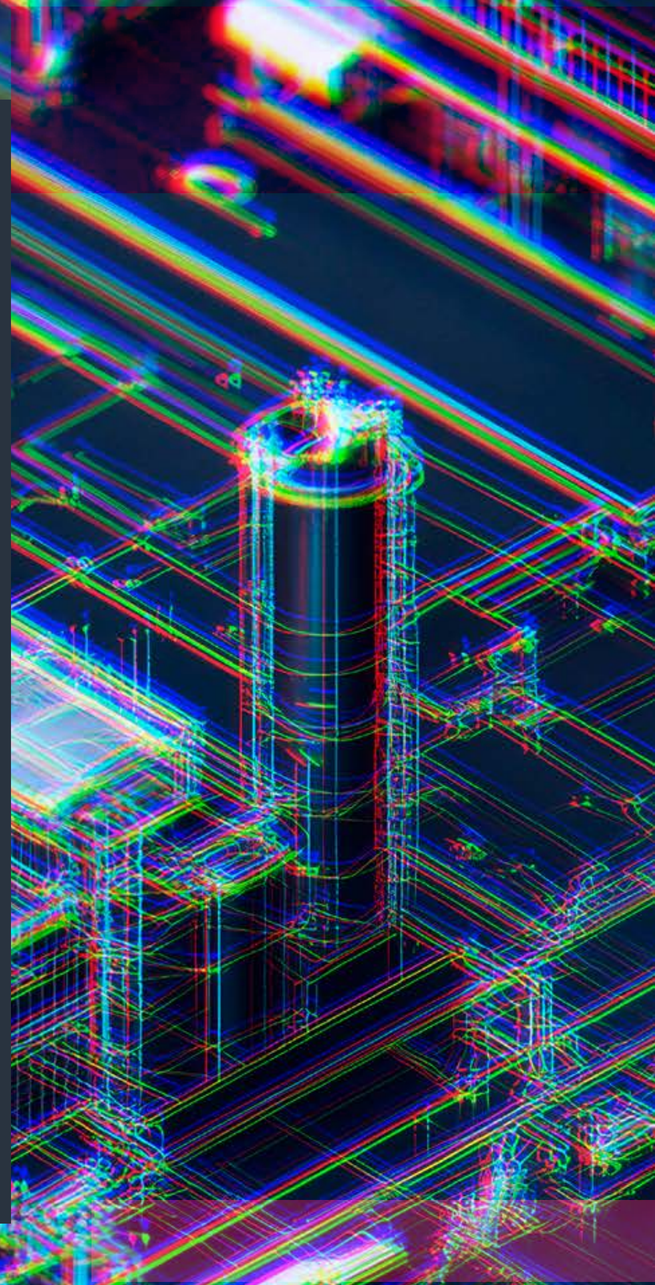
# Resumen ejecutivo

El informe sobre riesgos de VPN de Zscaler ThreatLabz 2025 ofrece una visión incisiva de la evolución de los riesgos asociados a las redes privadas virtuales (VPN) y subraya el cambio urgente hacia arquitecturas Zero Trust a medida que las organizaciones se esfuerzan por satisfacer las demandas de seguridad a prueba de futuro. Antiguamente consideradas como la columna vertebral del acceso remoto, las VPN se han convertido cada vez más en focos de ciberamenazas, pasando de ser herramientas esenciales a importantes riesgos de seguridad para las organizaciones de todo el mundo. Este informe, elaborado a partir de las opiniones de más de 600 profesionales de TI y seguridad, revela un cambio crítico en el panorama de la ciberseguridad: **más de la mitad de las organizaciones encuestadas experimentaron ataques debidos a vulnerabilidades de las VPN solo en el último año,** lo que pone de manifiesto la imperiosa necesidad de un nuevo enfoque en los entornos de trabajo actuales, cada vez más híbridos.

En 2025, la insatisfacción con las VPN tradicionales ha impulsado un cambio, y las empresas reconocen mayoritariamente que corregir estas vulnerabilidades es una carrera que ya no pueden ganar. Esta toma de conciencia impulsa la adopción generalizada de modelos Zero Trust, que prometen un control de acceso granular y reducen significativamente los riesgos de seguridad. Cabe destacar que **el 81 % de las organizaciones están implementando estrategias Zero Trust para 2026, y el 65 % planea eliminar por completo las VPN en el mismo período.** Además, las frustraciones operativas, como conexiones lentas, desconexiones frecuentes y procesos de autenticación complejos, han aumentado la urgencia, impulsando un aumento en la demanda de soluciones Zero Trust que garanticen un acceso fluido y seguro.

Todos estos cambios se producen en el contexto de un panorama de amenazas facilitado por la IA. De hecho, el aumento de los ciberataques impulsados por IA afectará la seguridad de las VPN de maneras nunca antes vistas. Los atacantes utilizarán cada vez más la IA para el reconocimiento automatizado de las vulnerabilidades de las VPN, que se escanean fácilmente a través de Internet público. Técnicas como la pulverización inteligente de contraseñas y el desarrollo rápido de exploits permitirán a los actores malintencionados comprometer las credenciales VPN a mayor escala. Más abajo en la cadena de ataque, las técnicas de evasión potenciadas por la IA dificultarán aún más la detección de intrusiones basadas en VPN antes de que se produzcan daños significativos. A medida que crezcan estas amenazas impulsadas por la IA, los riesgos de las VPN no harán sino aumentar, impulsando a las empresas a adoptar medidas de seguridad proactivas y acelerando el cambio, ya pronunciado, hacia soluciones Zero Trust.

Al reconocer estos cambios, el informe de ThreatLabz no solo traza el declive de las redes privadas virtuales, que han pasado de ser herramientas indispensables a convertirse en pasivos, sino que también proporciona ideas procesables para las empresas que navegan por este panorama transformador.




©2025 Zscaler, Inc. Todos los derechos reservados.

# Hallazgos clave

1. **La obsolescencia de las VPN se acelera:**

   Un importante 65 % de las empresas van a sustituir sus servicios VPN en el próximo año, lo que supone un aumento del 23 % con respecto a 2024. Esta tendencia está impulsada principalmente por la incapacidad de las VPN para satisfacer las exigencias de seguridad y cumplimiento de las empresas modernas, lo que pone de relieve su papel en la exacerbación de los riesgos en lugar de mitigarlos.

2. **Escalada de ciberataques explotados mediante VPN y amenazas de ransomware:**

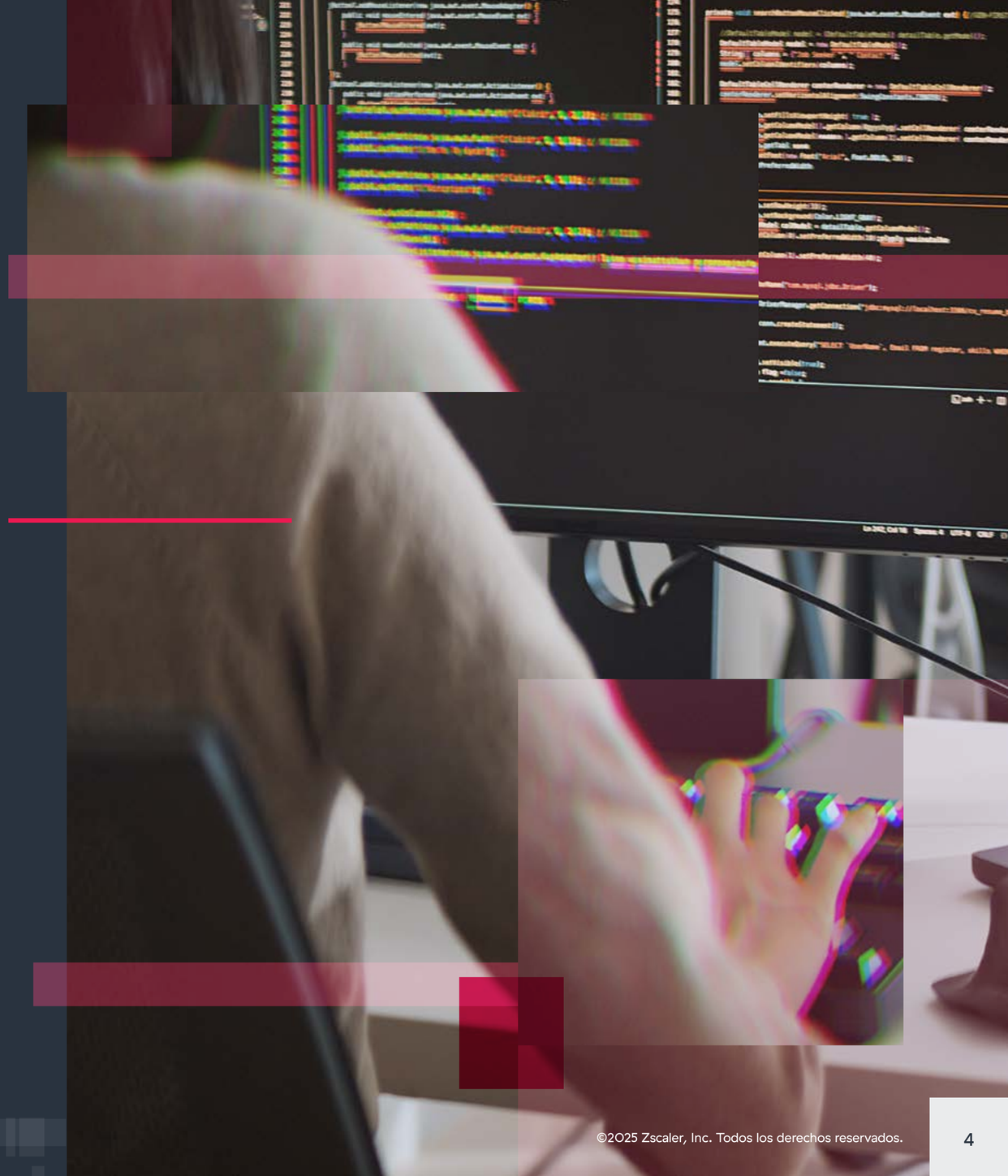
   El año pasado se produjo un aumento preocupante de los ciberincidentes relacionados con las vulnerabilidades de las VPN, ya que el 56 % de las organizaciones informaron de este tipo de violaciones, lo que supone un aumento alarmante con respecto a las cifras anteriores. Mientras tanto, al 92 % de los encuestados les preocupa que las vulnerabilidades de las VPN no parcheadas conduzcan directamente a ataques de ransomware. Estos hallazgos confirman la tendencia de que, ante la dificultad de aplicar parches a las vulnerabilidades de manera rápida, las empresas necesitan una revisión en profundidad de la seguridad para cubrir estas brechas de seguridad críticas y mitigar los riesgos siempre presentes de la explotación de las VPN.

3. **La insatisfacción del usuario final influye en la redirección de la seguridad:**

   Las frustraciones de los usuarios por las ineficiencias de las VPN (que van desde la lentitud hasta las autenticaciones engorrosas, complejas o defectuosas) influyen cada vez más en las estrategias de las organizaciones. Este descontento de los usuarios finales está impulsando el avance hacia arquitecturas Zero Trust que ofrecen un acceso ininterrumpido y seguro sin las molestias tradicionales asociadas a las VPN.

4. **La transición de la VPN a Zero Trust: del concepto a la implementación:**

   Como reflejo de un importante cambio estratégico, el 81 % de las organizaciones están avanzando activamente hacia la implementación de marcos Zero Trust en el próximo año. Esto marca una transición fundamental desde considerar Zero Trust como un ideal teórico a reconocerla como una necesidad práctica para sustituir a las VPN y mejorar al mismo tiempo la seguridad en entornos informáticos dinámicos y distribuidos.





©2025 Zscaler, Inc. Todos los derechos reservados.

# Riesgos de las VPN: ¿Por qué el 81% de las organizaciones adoptarán Zero Trust para 2026?

Las VPN se diseñaron para proporcionar acceso remoto, pero los tiempos han cambiado... y también los atacantes. Actualmente, las VPN sirven a menudo como puntos de entrada para ataques de ransomware, robo de credenciales y ciberespionaje debido a vulnerabilidades que son difíciles de parchear rápidamente; modelos de confianza implícitos que proporcionan un acceso completo a la red; y permisos de acceso generalizados. En conjunto, las vulnerabilidades de seguridad son el mayor desafío al que se enfrentan las empresas con respecto a las VPN (según el 54 % de los encuestados), lo que subraya el hecho de que los atacantes aprovechan habitualmente las fallas sin parchear o eluden las protecciones para infiltrarse en las redes.

Los riesgos se acentúan aún más con el acceso a VPN por parte de terceros. Un abrumador 93 % de los encuestados expresa su preocupación por las vulnerabilidades de puerta trasera introducidas por conexiones VPN externas, ya que los atacantes explotan cada vez más las credenciales de terceros para penetrar en las redes sin ser detectados. Tampoco se trata solo del acceso inicial: las VPN también hacen que las violaciones sean más destructivas. A diferencia de las soluciones Zero Trust que aplican políticas granulares para impedir el movimiento dentro de las redes, las VPN proporcionan un acceso amplio, lo que permite a los atacantes moverse lateralmente y escalar privilegios. En general, el 71 % de los encuestados identifican el movimiento lateral como una de las principales preocupaciones, reconociendo cómo amplifica el alcance y el impacto de una violación.

Estos desafíos, unidos a preocupaciones cotidianas como el rendimiento lento, la autenticación compleja y las desconexiones frecuentes, dejan claro por qué las empresas están dejando de lado las VPN para favorecer los modelos Zero Trust. El informe sobre riesgos de las VPN 2025, basado en las opiniones de 632 profesionales de TI y ciberseguridad, busca arrojar luz sobre el estado del uso de las VPN en 2025 para comprender mejor los riesgos y desafíos, así como ofrecer a las empresas una guía de mejores prácticas para mejorar su postura de ciberseguridad y su enfoque del acceso remoto seguro.

Las conclusiones de este informe ofrecen a los responsables de TI y de seguridad una visión fundamentada en datos sobre las razones para retirar las anticuadas VPN y adoptar una arquitectura Zero Trust moderna en la nube. El cambio de la confianza implícita a la verificación continua ya no es opcional: es esencial para proteger las empresas distribuidas de la actualidad, reducir la complejidad informática y garantizar una experiencia de usuario sin fisuras.





©2025 Zscaler, Inc. Todos los derechos reservados.

# Preocupaciones sobre la seguridad de las VPN

## La obsolescencia de las VPN: riesgos de seguridad y frustraciones de los usuarios

Las organizaciones que siguen confiando en las VPN para el acceso remoto se encuentran cada vez más expuestas a brechas de seguridad, ineficiencias operativas y una creciente insatisfacción de los usuarios finales, lo que refuerza el creciente sentimiento de que las VPN han quedado en el pasado de la seguridad de acceso.

El principal desafío, que son los riesgos de seguridad y cumplimiento, citados por el 54 % de los encuestados, refuerza la vulnerabilidad crítica de las VPN frente al ransomware, la escalada de privilegios y el movimiento de ataques laterales. Los atacantes ven las VPN como eslabones débiles listos para ser explotados, mientras que las organizaciones tienen dificultades para parchear estos sistemas obsoletos con la rapidez suficiente para mantenerse al día frente a las amenazas avanzadas.

La frustración de los usuarios ha llegado a su punto álgido: el 51 % de los encuestados identifican el bajo rendimiento de las VPN (incluidos elementos como la lentitud de la conectividad, las caídas y los engorrosos protocolos de autenticación) como un obstáculo para la productividad. Las VPN siguen siendo una carga operativa, ya que el 41 % de los encuestados citan dificultades en la gestión y el 37 % señalan los elevados costos del mantenimiento continuo. Estas cifras ilustran lo intensivas a nivel de recursos que se han vuelto las VPN, agotando los presupuestos de TI y obligando a los equipos a dedicar un tiempo innecesario a tareas repetitivas de solución de problemas.

### Fuera con los enfoques heredados, dentro con Zero Trust

Una violación reciente sirve como duro recordatorio de las vulnerabilidades de las VPN. En enero de 2025, un grupo de ciberespionaje chino explotó con éxito un día cero en la VPN Pulse Secure de Ivanti, permitiendo el acceso no autorizado a través de las redes corporativas. Este ataque, uno de tantos dirigidos a la tecnología VPN en los últimos meses, pone de relieve por qué las organizaciones ya no pueden darse el lujo de confiar en los modelos de acceso heredados para defender sus infraestructuras.

Ante estos desafíos, numerosos proveedores de VPN heredadas han empezado a calificar las máquinas virtuales suministradas a través de la nube como soluciones Zero Trust. Sin embargo, los servicios de VPN alojados en la nube siguen siendo fundamentalmente los mismos desde una perspectiva arquitectónica: son servicios conectados a Internet con una dirección IP pública que puede ser vulnerada.

**La eliminación de las dependencias de las VPN ya no es una mejora opcional, sino una necesidad inmediata. Las organizaciones necesitan hacer la transición a verdaderos marcos Zero Trust que ofrezcan un acceso basado en la identidad, con privilegios mínimos y una segmentación granular. Estas arquitecturas en la nube ayudan a reducir las superficies de ataque lateral, mejoran las experiencias de los usuarios y reducen drásticamente la complejidad de TI, una tríada de ventajas que las VPN sencillamente no pueden igualar.**

**¿Cuáles considera que son los mayores desafíos de sus soluciones VPN?**

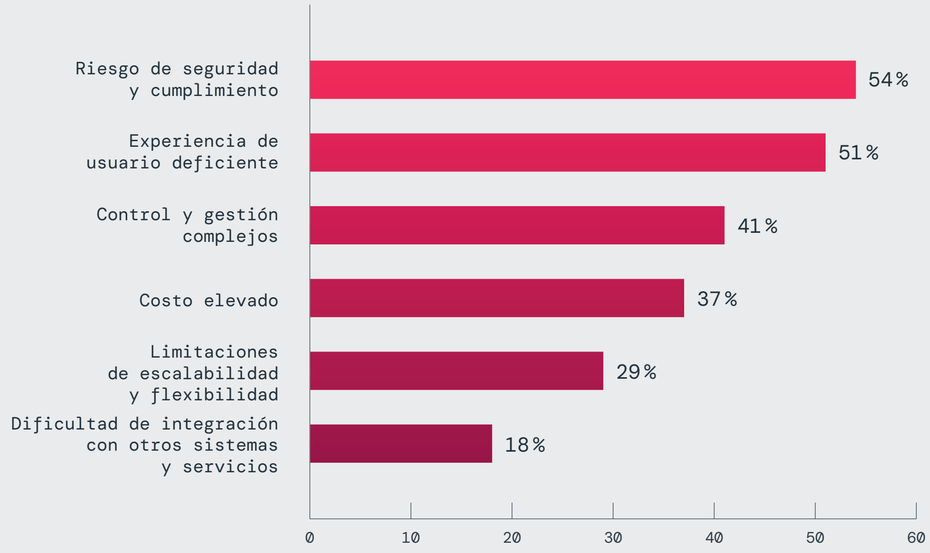



**Figura 1:** Los mayores desafíos de las soluciones VPN.


©2025 Zscaler, Inc. Todos los derechos reservados.

Un ejemplo concreto: la industria ha sido testigo recientemente de picos masivos en la actividad de escaneado dirigida a más de veinte mil direcciones IP de VPN públicas alojadas por uno de los mayores proveedores de seguridad. Históricamente, este tipo de actividad ha indicado cierta probabilidad de que los atacantes se estén preparando para explotar vulnerabilidades aún no reveladas en activos VPN específicos. En otras palabras: si usted es localizable, es vulnerable. Por ello, desde una perspectiva arquitectónica, la tecnología VPN basada en la nube nunca podrá alcanzar los verdaderos principios Zero Trust, independientemente de cómo se venda.

## Ransomware y VPN: una tormenta perfecta de riesgos

Los grupos de ransomware siguen explotando las vulnerabilidades de las VPN con una precisión devastadora, aprovechando tanto las fallas de día cero como las debilidades conocidas antes de que las organizaciones puedan implementar los parches de seguridad. Las VPN se han convertido en un blanco fácil para los atacantes debido a su adopción generalizada y su dependencia de modelos de confianza de red obsoletos.

En general, el 92 % de los encuestados expresaron un alto nivel de preocupación por el ransomware dirigido a vulnerabilidades de VPN sin parches, lo que pone de relieve la necesidad crítica de mecanismos de protección más robustos. Estos datos subrayan por qué las VPN se consideran ahora como pasivos más que como herramientas confiables para mitigar los ciberriesgos modernos.

Los ejemplos del mundo real continúan validando estos temores. En enero de 2023, varias organizaciones sanitarias estadounidenses fueron víctimas de un ataque de ransomware provocado por una vulnerabilidad no parcheada de Citrix NetScaler (CVE-2023-4966). Este exploit permitió a los atacantes infiltrarse en los sistemas, interrumpir el funcionamiento de los hospitales, bloquear los historiales de los pacientes y obligar a los centros a desviar la atención de urgencias críticas, todo ello porque la vulnerabilidad no se había parcheado a tiempo.  Este incidente subraya el riesgo generalizado que suponen las VPN sin parchear. Los malintencionados escanean regularmente los sistemas expuestos, asegurándose de que pueden capitalizar las vulnerabilidades antes de que las organizaciones las corrijan, dejando a las organizaciones en riesgo de verse comprometidas, sufrir interrupciones operativas y pérdidas financieras.

**Las organizaciones deben acabar con el ciclo interminable de parches y adoptar estrategias defensivas proactivas adaptadas a la evolución de las amenazas. Los marcos Zero Trust dan prioridad al control de acceso basado en la identidad y a la verificación continua, lo que garantiza una importante reducción del riesgo de ransomware, incluso cuando las vulnerabilidades siguen sin parchearse. Los sistemas de detección automatizados y las políticas dinámicas contienen aún más las posibles violaciones, impidiendo que los atacantes se desplacen lateralmente o escalen privilegios.**

**¿Hasta qué punto le preocupa ser blanco de ransomware debido a vulnerabilidades sin parchear?**

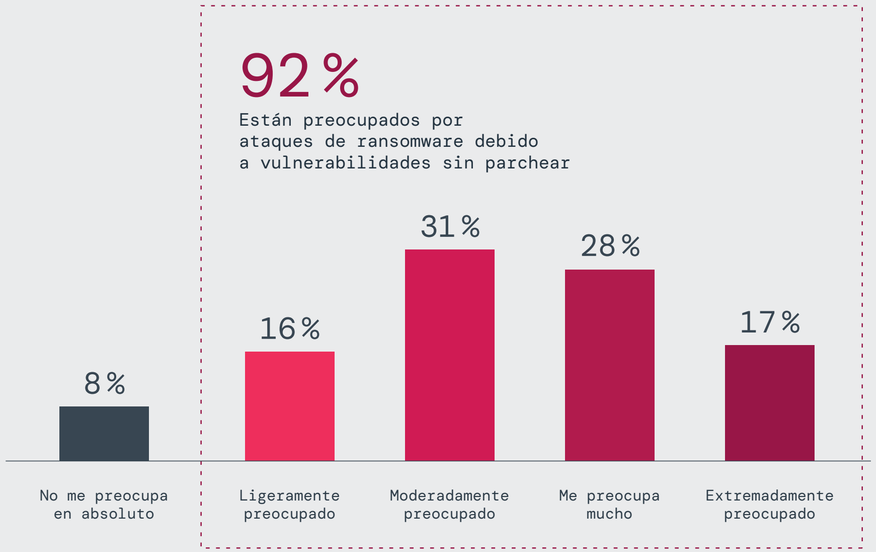



**Figura 2:** Preocupaciones sobre ataques de ransomware.


©2025 Zscaler, Inc. Todos los derechos reservados.

# VPN y movimiento lateral: aumento del radio de alcance de las violaciones

Además de permitir el compromiso inicial a través de ransomware y otras amenazas, las VPN facilitan el movimiento lateral, una técnica de ataque peligrosa. Los atacantes aprovechan el amplio acceso que proporcionan las VPN para escalar privilegios e infiltrarse más profundamente en las redes objetivo, a menudo con consecuencias devastadoras.

Un total del 71 % de los encuestados expresó cierto nivel de preocupación por este riesgo, y un 32 % expresó un alto nivel de preocupación. Estos sentimientos están justificados, ya que las VPN suelen conceder un amplio acceso a la red, lo que permite a los atacantes pasar desapercibidos, escalar privilegios y exfiltrar datos confidenciales una vez dentro.

En septiembre de 2024, los atacantes explotaron múltiples vulnerabilidades de día cero en Cloud Service Appliance (CSA) de Ivanti, en particular CVE-2024-8963 y CVE-2024-8190, para vulnerar varias organizaciones, tal y como confirmaron la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) y el FBI. Los atacantes eludieron los controles administrativos, ejecutaron comandos arbitrarios, cosecharon credenciales e implantaron web shells, permitiendo el movimiento lateral a través de las redes. A pesar de los incidentes de seguridad anteriores relacionados con las VPN de Ivanti, estos nuevos exploits demuestran que parchear o rediseñar las soluciones VPN heredadas sigue sin solucionar las fallas de seguridad fundamentales inherentes a los modelos de acceso remoto basados en la red.

**¿Qué tan preocupado está usted de que los atacantes se desplacen lateralmente a través de su red si una VPN se ve comprometida?**

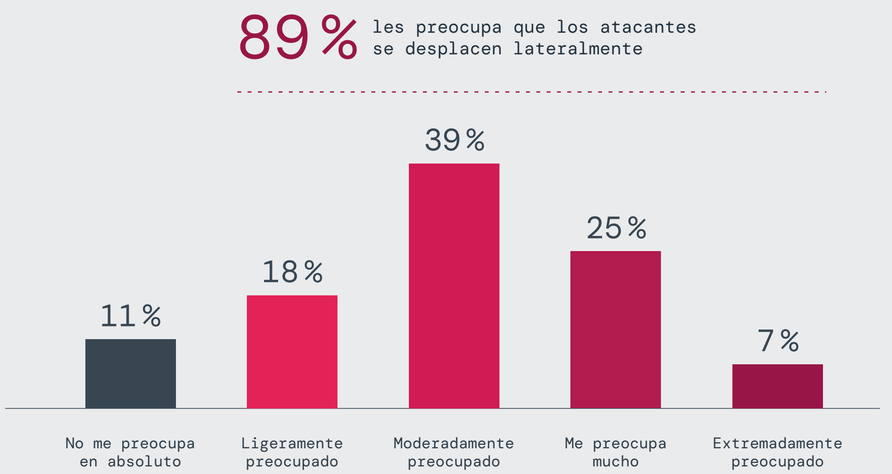



**Figura 3:** Preocupaciones empresariales que se desplazarán lateralmente por la red si una VPN se ve comprometida.

**Para mitigar estos riesgos, las organizaciones deben pasar de un acceso basado en VPN a un acceso a la red Zero Trust (ZTNA) con una segmentación estricta. A diferencia de las VPN, que conceden a los usuarios un amplio acceso a la red, ZTNA proporciona un acceso a nivel de aplicación basado en la identidad y el contexto, garantizando que los usuarios sólo puedan acceder a los recursos específicos que necesitan. Este enfoque impide el movimiento lateral incluso si los atacantes consiguen el acceso inicial, reduciendo drásticamente la superficie de ataque y el radio potencial de alcance de las violaciones. Además, la implementación de la red y la microsegmentación refuerza la seguridad al aislar los sistemas críticos e impedir la comunicación no autorizada entre los activos comprometidos y los seguros.**


©2025 Zscaler, Inc. Todos los derechos reservados.

# CVE de VPN de 2020 a 2025: una ola creciente de vulnerabilidades de alta gravedad

Ningún software es inmune a las vulnerabilidades de seguridad, ni debe esperarse que lo sea. Sin embargo, en el caso de la tecnología VPN, las vulnerabilidades, en particular las amenazas de día cero, pueden ser especialmente perjudiciales, ya que los malintencionados pueden sondear fácilmente la infraestructura VPN afectada y explotarla antes de que se publique o se haya aplicado ningún parche. Los informes de CVE son positivos, ya que este esfuerzo de toda la comunidad ayuda a vendedores y clientes a seguir las mejores prácticas y mejorar su ciberhigiene mediante la aplicación de parches y la divulgación. La manera en que se descubren estos CVE y la información que contienen reflejan los cambios en el panorama de las amenazas en evolución.

Zscaler ThreatLabz analizó 411 vulnerabilidades y exposiciones comunes (CVE) de VPN entre 2020 y 2025, según lo informado por el Programa de CVE de MITRE. Los resultados indican un aumento de vulnerabilidades de VPN que han aumentado gradualmente durante la primera mitad de esta década. Estos CVE cubren una amplia variedad de fallas de VPN, desde la explotación de interfaces de administración basadas en web a través de la inyección de comandos y vulnerabilidades de validación de entrada, hasta fallas criptográficas y ataques DoS y DDoS. No faltan vulnerabilidades recientes de VPN, muchas de las cuales han provocado violaciones de seguridad importantes y muy visibles.

Muchas de estas CVE son críticas. En 2024, por ejemplo, el 60 % de las 83 vulnerabilidades de VPN notificadas por el NIST indicaron una puntuación CVSS alta o crítica. Mientras tanto, las vulnerabilidades de ejecución remota de código (RCE), que permiten a los atacantes ejecutar comandos arbitrarios y potencialmente comprometer el sistema, fueron las CVE de VPN más comunes. En otras palabras, lejos de ser inocuas, la mayoría de las CVE de VPN del año pasado dejaron a sus usuarios extremadamente vulnerables a exploits que los atacantes ejecutan con relativa facilidad. Además, muchos de estos CVE eran exploits de día cero. Aunque las CVE de 2025 siguen siendo escasas a principios de año, ya se han revelado vulnerabilidades importantes, como dos exploits de día cero, CVE-2025-0282 y CVE-2025-0283.

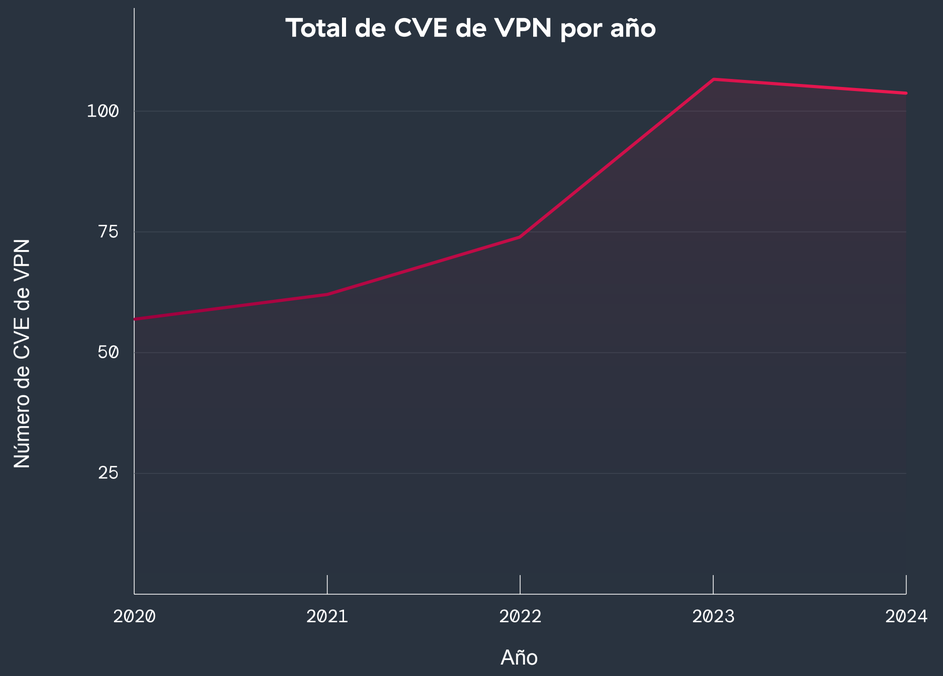



**Figura 4:** Total de CVE de VPN para cada año, de 2020 a 2024.


©2025 Zscaler, Inc. Todos los derechos reservados.

## 1. Las RCE siguen siendo la principal amenaza

- **Observación:** Las vulnerabilidades RCE encabezan la lista en los cuatro años, con 32 solo en 2024. La RCE representa 149 CVE incluidos los datos de 2025, lo que la convierte en el tipo de vulnerabilidad más frecuente y crítica.
- **Implicación:** Las vulnerabilidades de RCE permiten a los atacantes ejecutar comandos arbitrarios en dispositivos VPN, lo que podría comprometer por completo el sistema. Las empresas deben priorizar la aplicación de parches y la protección de los sistemas vulnerables a estos exploits.

## 2. La escalada de privilegios crece constantemente con el tiempo

- **Observación:** Hay un aumento constante en los CVE de escalada de privilegios (66.7 %), alcanzando su punto máximo en 2024 con 20 vulnerabilidades.
- **Implicación:** Los atacantes explotan cada vez más las vulnerabilidades de las VPN para escalar privilegios y obtener así el control administrativo de los sistemas. Las empresas deben garantizar la seguridad de las configuraciones de los sistemas y restringir estrictamente el acceso a los privilegios.

## 3. Las vulnerabilidades por denegación de servicio (DoS) registran un fuerte aumento del 200 %

- **Observación:** Los CVE relacionados con DoS se triplicaron de 9 en 2020 a 27 en 2024, convirtiéndose en el segundo tipo de mayor impacto en los últimos años: 85 CVE en total, incluidos los datos de 2025 hasta el momento.
- **Implicación:** Los ataques DoS son cada vez más sofisticados, lo que convierte a los sistemas VPN en objetivos prioritarios para las interrupciones operativas. Las empresas deberían implementar la limitación de velocidad y el modelado de tráfico para mitigar estos riesgos.

## 4. La fuga de información confidencial es menos frecuente, pero sigue siendo crítica

- **Observación:** Aunque son relativamente menos comunes, con 41 CVE en total, las vulnerabilidades de filtración de información confidencial exponen credenciales críticas, claves de cifrado y datos de usuario.
- **Implicación:** Este tipo de impacto es particularmente perjudicial para la confidencialidad y el cumplimiento normativo. Las empresas deben implementar un cifrado robusto, prácticas de codificación seguras y monitorización del tráfico para detectar y prevenir la fuga de datos.

## 5. Crecimiento constante de las vulnerabilidades de elusión de autenticación

- **Observación:** Los incidentes de elusión de autenticación han sido relativamente bajos, pero consistentes, creciendo de 4 en 2020, a un pico de 6 en 2023, a 4 vulnerabilidades en 2024 – sumando un total de 30 CVE a lo largo del tiempo:
- **Implicación:** Los atacantes se están aprovechando de las vulnerabilidades de la autenticación multifactor (MFA) y la lógica de inicio de sesión para suplantar la identidad de los usuarios. Las empresas deben reforzar las configuraciones de MFA y supervisar los comportamientos de inicio de sesión anormales.

# Tendencias clave: Tipos de impacto de las CVE

Para comprender el daño potencial de estas vulnerabilidades si fueran explotadas, ThreatLabz evaluó las CVE de VPN en cinco categorías de ataque: ejecución remota de código (RCE), escalada de privilegios, filtración de información, denegación de servicio (DoS) y elusión de autenticación. Tenga en cuenta que algunas categorías son agrupaciones generales para tipos de ataques distintos, pero estrechamente relacionados: por ejemplo, la elusión de la autenticación incluye ataques que pueden eludir el segundo factor o la autenticación multifactor (MFA), mientras que otros eluden las medidas de autenticación básica. En general, cualquier vulnerabilidad de RCE será un elemento de alta prioridad a remediar para cualquier organización.

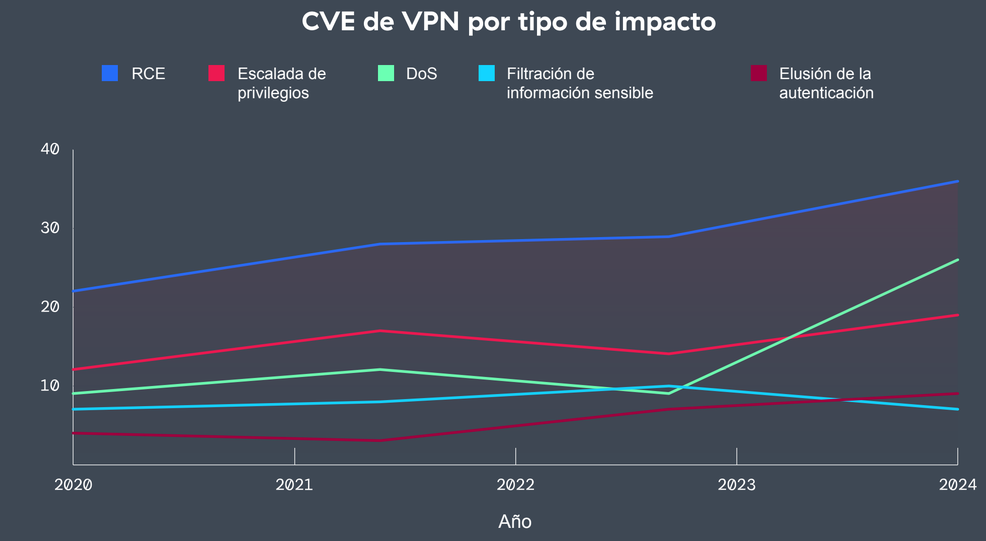



**Figura 5:** El tipo de impacto de las CVE de VPN entre 2020 y 2024, que abarcan RCE, escalada de privilegios, DoS, fuga de información confidencial, elusión de autenticación.


©2025 Zscaler, Inc. Todos los derechos reservados.

# Tendencias clave: vulnerabilidades críticas de VPN

Más allá de los tipos de impacto, ThreatLabz también analizó la gravedad de las CVE de VPN cada año. **En general, ThreatLabz descubrió que las CVE con puntuaciones CVSS ALTA o CRÍTICA crecieron un 38.9 % de 2020 a 2024.** De hecho, el 66.3 % de todas las CVE en el año 2024 fueron calificadas como ALTA o CRÍTICA, lo que indica un impacto potencial grave para las organizaciones cuando dichas CVE son explotadas antes de que sean parcheadas. Además, ThreatLabz analizó las tendencias críticas en los diferentes tipos de vulnerabilidades representadas en los datos de CVE que las empresas deberían comprender para defenderse mejor contra las amenazas VPN en evolución.

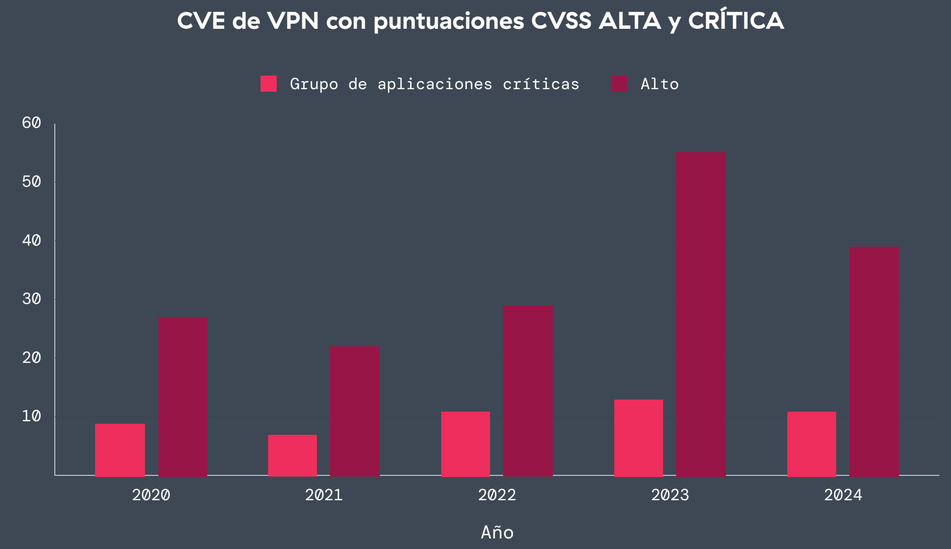



**Figura 6:** El volumen de CVE de VPN con puntuaciones CVSS ALTAS y CRÍTICAS de 2020 a 2024.

## 1. Aumento de la explotación de las interfaces de gestión basadas en la web

- **Tendencia:** Las vulnerabilidades de inyección de comandos y validación de entradas han aumentado constantemente, lo que indica que los atacantes se centran cada vez más en los portales administrativos y de gestión, tanto desde la perspectiva del administrador como del usuario final. Como estas interfaces están intrínsecamente expuestas a Internet a través de su arquitectura, son propensas a ser explotadas por los malintencionados.
- **Escalada:** Aunque estas vulnerabilidades estaban presentes en 2020–2021, se intensificaron significativamente a partir de 2022, lo que sugiere que los atacantes ven estas interfaces de gestión como objetivos atractivos y accesibles, especialmente debido a prácticas de codificación de seguridad inadecuadas.

## 2. Autenticación generalizada y elusiones de MFA

- **Tendencia:** Los ataques dirigidos específicamente a los métodos de autenticación (incluidas las elusiones de MFA, el secuestro de sesiones y la gestión inadecuada de sesiones) aumentaron constantemente.
- **Escalada:** En los primeros años (2020–2021) principalmente se produjeron elusiones de autenticación más sencillas, mientras que a partir de 2023–2025, estas evolucionaron hacia ataques más avanzados, automatizados y persistentes dirigidos explícitamente a las debilidades de la MFA, lo que indica la intención de los atacantes de socavar medidas de seguridad más fuertes.

## 3. Aumento de los exploits locales de escalada de privilegios

- **Tendencia:** Las vulnerabilidades locales de escalada de privilegios se han vuelto más frecuentes y cada vez más graves.
- **Escalada:** Lo que comenzó como pequeños descuidos de configuración en 2020–2021 se intensificó en 2024–2025 hasta convertirse en métodos de escalada de privilegios más sofisticados, como el secuestro de DLL, que proporciona a los atacantes un acceso más profundo a nivel de sistema.


©2025 Zscaler, Inc. Todos los derechos reservados.

## 4. Creciente sofisticación de los ataques DoS y DDoS

- **Tendencia:** Los ataques DoS evolucionaron desde el agotamiento básico de recursos (2020–2021) a sofisticadas técnicas de amplificación DDoS (2024–2025).
- **Escalada:** Los atacantes pasaron de simples interrupciones basadas en paquetes malformados a ataques amplificados más avanzados, lo que refleja una escalada estratégica para maximizar la interrupción operativa.

## 5. Fallas criptográficas persistentes e intensificadas

- **Tendencia:** Los problemas relacionados con la implementación criptográfica (como validación incorrecta de certificados, claves fugadas y verificación TLS insuficiente) han aumentado notablemente.
- **Escalada:** A partir de 2022, se observó un aumento notable de vulnerabilidades criptográficas, alcanzando su punto máximo entre 2024 y 2025 con fallas de alta gravedad. Este aumento demuestra el interés estratégico de los adversarios en explotar las debilidades del cifrado para socavar la confidencialidad de las VPN.




©2025 Zscaler, Inc. Todos los derechos reservados.

# sobre la seguridad de las VPN (cont.)

## Los desafíos de aplicar la segmentación

Dados los riesgos del movimiento lateral, muchas organizaciones intentan limitar la propagación de los ataques mediante la segmentación. Si bien la segmentación es un mecanismo de defensa fundamental para reducir la superficie de ataque, su implementación suele ser un desafío.

La encuesta destaca estos desafíos, ya que el 51 % de las organizaciones prevén o se enfrentan a la complejidad de la configuración. Además, el 39 % informa de una falta de experiencia y recursos, mientras que el 24 % se enfrenta a cuellos de botella en el rendimiento, lo que indica que las arquitecturas de red heredadas están mal equipadas para sustentar los controles de acceso granulares que requieren los entornos de TI actuales.

Los problemas de segmentación desempeñaron un papel notable en el ataque de ransomware a MGM Resorts en 2023, en el que los atacantes obtuvieron un acceso inicial mediante ingeniería social, pero pudieron desplazarse lateralmente debido a una segmentación insuficiente. La violación interrumpió las operaciones de los hoteles, los cajeros automáticos y los sistemas de juego de los casinos, lo que costó a la empresa unos daños estimados en 100 millones de dólares. Este caso pone de relieve cómo una segmentación deficiente permite a los atacantes pivotar por los sistemas críticos, amplificando el impacto de una intrusión inicial.

**Para hacer frente a estos desafíos, las organizaciones deben implantar modelos de segmentación basados en la nube y basados en la identidad que agilicen la aplicación de las políticas y reduzcan la sobrecarga manual. A diferencia de la segmentación de red tradicional, que se basa en complejas reglas de firewalls y configuraciones de VLAN, un enfoque Zero Trust permite una segmentación dinámica basada en la identidad de los usuarios, la postura de los dispositivos y las evaluaciones de riesgos en tiempo real. Esto garantiza que solo los usuarios autorizados puedan acceder a aplicaciones específicas, al tiempo que se mantiene la seguridad de la red en general.**

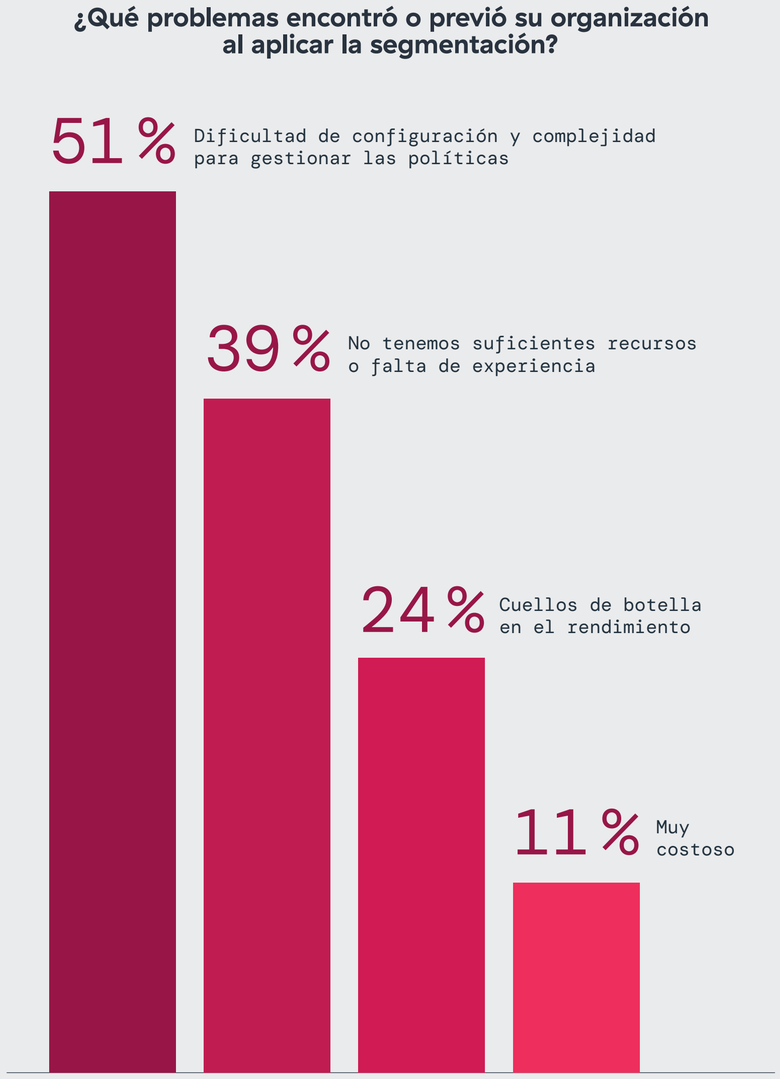



**Figura 7:** Los principales desafíos que enfrentan las empresas al implementar la segmentación.


©2025 Zscaler, Inc. Todos los derechos reservados.

# Las VPN aumentan los riesgos de ciberseguridad en las fusiones y adquisiciones

Más allá de los desafíos de seguridad cotidianos, las grandes transiciones informáticas, como las fusiones y adquisiciones, suponen riesgos adicionales y amplían las superficies de ataque. Estas transiciones suelen implicar la fusión de redes, aplicaciones e identidades dispares, lo que puede dar lugar a vulnerabilidades heredadas, configuraciones erróneas y controles de seguridad débiles.

Casi dos tercios (64 %) de los encuestados expresaron su preocupación por las ciberamenazas tras las fusiones y adquisiciones, reconociendo las brechas de seguridad que surgen durante las integraciones de TI.

Un ejemplo reciente es la violación de datos de Capita en 2023, donde los atacantes explotaron las debilidades de seguridad tras una adquisición corporativa, obteniendo acceso no autorizado a datos confidenciales. El incidente tuvo su origen en la desalineación de las políticas de seguridad entre las entidades fusionadas, lo que permitió a los actores de las amenazas desplazarse lateralmente por la red recién integrada. Esta violación pone de relieve cómo los controles de seguridad incoherentes, el acceso a VPN heredadas y los entornos no segmentados crean las condiciones ideales para los ciberataques durante la actividad de fusiones y adquisiciones.

**Para mitigar estos riesgos durante las fusiones y adquisiciones, las organizaciones deben dar prioridad a la diligencia debida en materia de ciberseguridad, aplicar el acceso con privilegios mínimos e implementar la segmentación. A diferencia de los modelos de acceso basados en VPN, Zero Trust impide que los entornos de TI fusionados hereden amplios permisos de acceso, lo que reduce eficazmente el riesgo de movimiento lateral y de escalada de privilegios. Al sustituir las VPN y las defensas basadas en el perímetro por controles de acceso basados en la identidad que validan cada solicitud, las organizaciones pueden asegurar tanto los entornos de TI heredados como los recién integrados.**

**¿Le preocupa ser vulnerable a ataques de ciberseguridad tras una fusión o adquisición?**

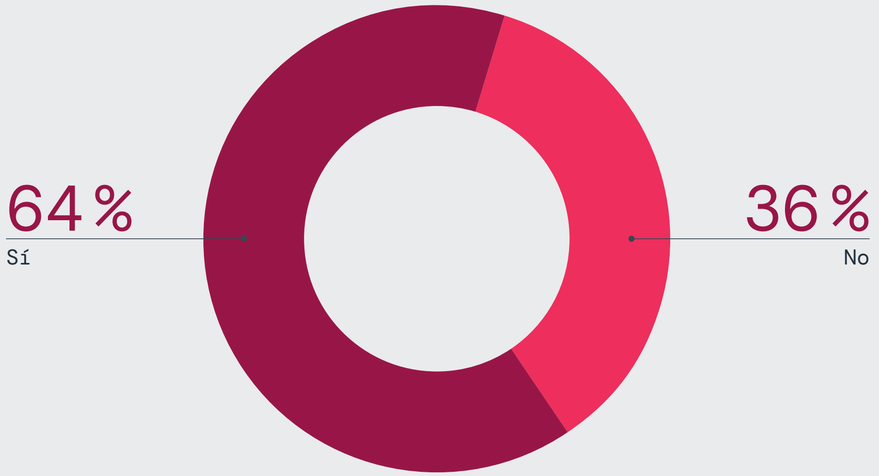



**Figura 8:** A las empresas les preocupan los ciberataques tras las fusiones y adquisiciones


©2025 Zscaler, Inc. Todos los derechos reservados.

# Acceso a VPN de terceros: Una puerta trasera para los atacantes

El acceso de terceros se ha convertido en uno de los puntos de entrada más vulnerables para los atacantes. Las VPN tradicionales, por diseño, cuentan con un amplio acceso a la red una vez completada la autenticación, extendiendo este privilegio a proveedores y socios externos. Esta práctica crea puntos ciegos que los atacantes están ansiosos por explotar. Los atacantes pueden aprovecharse de credenciales robadas o débiles, configuraciones erróneas y vulnerabilidades sin parchear para secuestrar estas conexiones de confianza. Teniendo en cuenta que el 93 % de los encuestados expresan una preocupación crítica por las vulnerabilidades de puerta trasera, el acceso de terceros representa una bomba de tiempo para las organizaciones que dependen de modelos de acceso estáticos y basados en la confianza.

Esta preocupación está bien fundada. En agosto de 2024, Enterprise Financial Group (EFG) sufrió una importante violación de datos que expuso la información personal de casi 20,000 clientes. La violación se rastreó hasta las vulnerabilidades de una VPN de terceros utilizada por EFG, que los atacantes explotaron para infiltrarse en la red y acceder a datos confidenciales. Este incidente subraya cómo las VPN de terceros crean brechas de seguridad que los atacantes pueden explotar como puntos de entrada a las redes corporativas.

**Las organizaciones deberían empezar por auditar el acceso a VPN de terceros y aplicar controles de políticas más estrictos, como el acceso limitado en el tiempo, la inspección del tráfico de extremo a extremo (del dispositivo a la aplicación) y la autenticación adaptable. La transición a un modelo Zero Trust permitirá hacer cumplir el acceso específico a las aplicaciones, garantizando que los socios externos solo tengan el acceso mínimo necesario. Además, la supervisión continua y las políticas basadas en el riesgo pueden mitigar significativamente las vulnerabilidades de terceros.**

**¿Hasta qué punto le preocupa que los terceros sirvan de posible puerta trasera para que los atacantes entren en su red a través de su acceso VPN?**

93 % le preocupa que entidades externas sirvan como potenciales puertas traseras a sus redes a través del acceso VPN

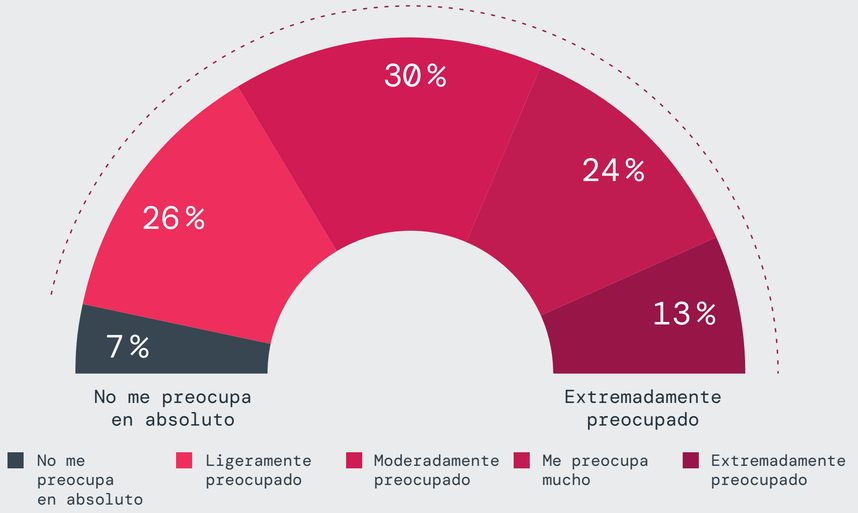



**Figura 9:** Preocupación de las empresas ante la posibilidad de que el acceso a VPN de terceros facilite los ciberataques.


©2025 Zscaler, Inc. Todos los derechos reservados.

# Desafíos y brechas de las medidas de protección heredadas

## Las herramientas tradicionales dejan al descubierto las aplicaciones privadas

Proteger las aplicaciones privadas contra las amenazas cada vez más sofisticadas basadas en la web (como el ransomware, el robo de credenciales y el abuso de API) se ha convertido en una prioridad fundamental para las empresas modernas. Sin embargo, muchas organizaciones siguen confiando en herramientas heredadas mal equipadas para contrarrestar el panorama actual de amenazas.

Según la encuesta, los firewalls (84 %), los firewalls de aplicaciones web (58 %) y las VPN (43 %) siguen dominando las defensas contra ataques web de las organizaciones. Sin embargo, los atacantes están eludiendo cada vez más estas herramientas (aprovechando los dispositivos sin parchear, las configuraciones deficientes y las debilidades inherentes a los modelos de seguridad basados en el perímetro), lo que demuestra que estas defensas heredadas ya no satisfacen las exigencias de los entornos de amenazas modernos.

Las recientes violaciones ponen de manifiesto las deficiencias de este tipo de defensas basadas en el perímetro. En agosto de 2024, hackers chinos (un grupo apodado Salt Typhoon) se infiltraron en importantes empresas de telecomunicaciones estadounidenses, como AT&T y Verizon, aprovechando vulnerabilidades en dispositivos de red y routers sin parchear. Este ataque comprometió metadatos confidenciales de más de un millón de usuarios, demostrando cómo los adversarios sofisticados pueden burlar medidas de seguridad tradicionales como firewalls y VPN.

**La única solución viable para proteger eficazmente las aplicaciones privadas es ir más allá de las anticuadas defensas perimetrales y adoptar modelos de acceso Zero Trust. Las arquitecturas Zero Trust eliminan la dependencia de la seguridad basada en la red, permitiendo a los usuarios conectarse directamente a las aplicaciones con políticas estrictamente aplicadas de acceso granular y con privilegios mínimos. A diferencia de los firewalls y las VPN, las arquitecturas Zero Trust permiten a los usuarios conectarse directamente a las aplicaciones con un acceso granular y de privilegios mínimos. Este enfoque bloquea los intentos de acceso no autorizados e impide el movimiento lateral, el secuestro de sesiones y el robo de credenciales, que son las tácticas que los atacantes suelen utilizar para burlar las defensas perimetrales tradicionales.**

**¿Qué productos utiliza para proteger sus aplicaciones privadas contra ataques basados en la web?**

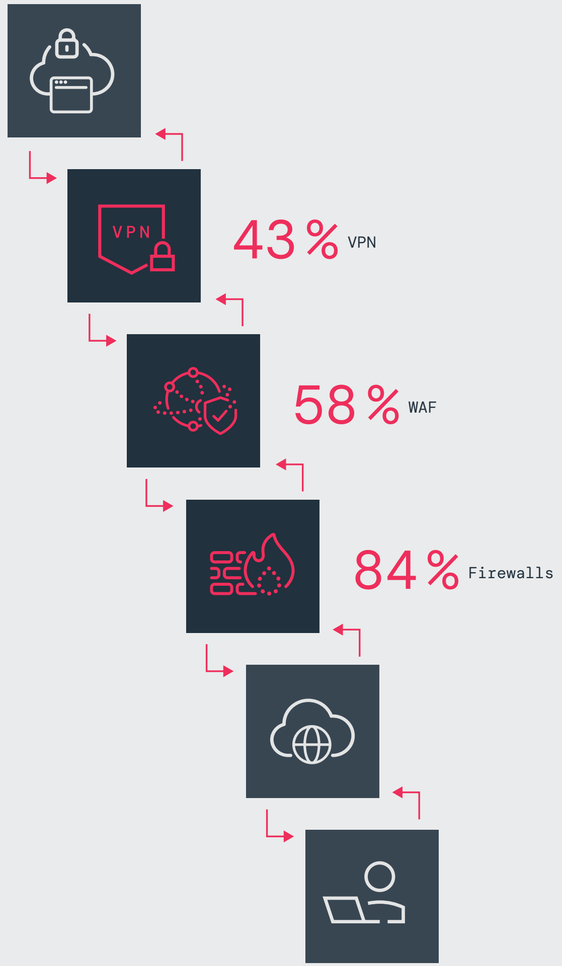



**Figura 10:** Los productos de seguridad que utilizan las empresas para defender sus aplicaciones privadas de las amenazas basadas en la web.


©2025 Zscaler, Inc. Todos los derechos reservados.

# Implementación de NAC en entornos VPN: una salvaguarda limitada

Un notable 54 % de las organizaciones encuestadas afirman utilizar el NAC para asegurar el acceso VPN a los recursos privados. Sin embargo, estas implementaciones aún no han evitado las violaciones y los exploits comúnmente asociados a las vulnerabilidades de las VPN, lo que subraya la incapacidad del NAC para abordar los riesgos sistémicos de los modelos de confianza basados en la red.

Las soluciones NAC refuerzan las verificaciones de la postura del dispositivo, la autenticación y la segmentación de la red. Sin embargo, no abordan los principales problemas de seguridad de las VPN, como los amplios permisos de acceso, los riesgos de movimiento lateral y la dependencia de la confianza implícita.

Las recientes violaciones demuestran que, incluso con NAC en funcionamiento, las vulnerabilidades de las VPN siguen siendo un punto débil crítico. En noviembre de 2023, el Departamento de Energía de los Estados Unidos confirmó un importante incidente de seguridad relacionado con credenciales VPN comprometidas, que permitieron a los atacantes saltarse los controles de acceso e infiltrarse en sistemas internos confidenciales. Esto destaca cómo los atacantes pueden explotar las debilidades de las VPN directamente, ya sea mediante el robo de credenciales, vulnerabilidades sin parchear o el secuestro de sesiones, lo que convierte al NAC en una defensa incompleta si el modelo de confianza subyacente permanece inalterado.

**¿Está utilizando un NAC (Control de acceso a red) entre su VPN y sus recursos privados?**

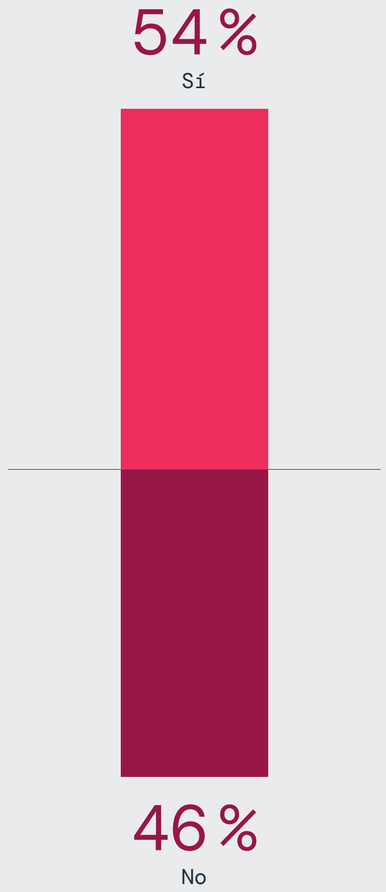



**Figura 11:** Proporción de empresas que utilizan NAC entre VPN y recursos privados.



**Para superar las limitaciones del NAC y de las arquitecturas VPN heredadas, las organizaciones deben adoptar un modelo de seguridad Zero Trust. Zero Trust elimina la confianza generalizada en la red al permitir que los usuarios se conecten directamente a aplicaciones específicas bajo políticas validadas continuamente y vinculadas a la identidad, la postura del dispositivo y el contexto. Zero Trust no solo bloquea el acceso no autorizado, sino que también impide el movimiento lateral, frustrando a los atacantes antes de que puedan escalar privilegios o exfiltrar datos.**


©2025 Zscaler, Inc. Todos los derechos reservados.

# Experiencia de usuarios de VPN y problemas de gestión

## El problema del rendimiento de las VPN: frustración de los usuarios y sobrecarga de TI

Las VPN no solo son una responsabilidad en términos de seguridad: también son una fuente importante de insatisfacción de los usuarios. Los usuarios finales expresan cada vez más su frustración por los problemas de rendimiento de las VPN, que crean obstáculos para la productividad y se suman a la creciente presión sobre los equipos de TI.

La lentitud de la conexión es la queja más común (23 %), lo que subraya la reputación de las VPN por su latencia, congestión y bajo rendimiento cuando se accede a aplicaciones en la nube desde casa. Los desafíos de autenticación también siguen siendo un problema importante, ya que el 20 % de los encuestados citan procesos de inicio de sesión complejos y el 17 % tiene problemas para acceder a las aplicaciones debido a errores de autenticación.

Estos problemas de rendimiento interrumpen las operaciones empresariales diarias, merman la productividad y convierten el servicio de asistencia de TI en un cuello de botella, ya que los equipos tienen que lidiar con las frecuentes solicitudes de solución de problemas, un problema que solo empeora a medida que los entornos de trabajo remotos e híbridos aumentan en complejidad.

**La sustitución de las VPN por el acceso a la red Zero Trust (ZTNA) no solo elimina la congestión del ancho de banda, sino que mejora enormemente la experiencia del usuario final al permitir conexiones directas, seguras y sin latencia a las aplicaciones. A diferencia de las VPN, que dirigen todo el tráfico a través de una puerta de enlace central y crean cuellos de botella en el rendimiento, ZTNA permite un acceso directo y seguro a las aplicaciones sin degradación del rendimiento. Mediante la adopción de controles de acceso basados en la identidad, la verificación continua y la seguridad proporcionada por la nube, las organizaciones no solo pueden eliminar las frustraciones comunes de las VPN, sino también aumentar la productividad de la fuerza de trabajo y reducir la carga informática que supone la resolución de problemas y el soporte de marcos VPN inflexibles.**

**¿Cuál es la queja más común de sus usuarios cuando acceden a las aplicaciones a través de una VPN?**



23 % Velocidad de conexión lenta al acceder a las aplicaciones

20 % Proceso de autenticación de VPN complejo o con dificultades

17 % Dificultad para acceder a las aplicaciones debido a problemas de autenticación

14 % Problemas con las caídas de conexión al utilizar VPN

13 % Experiencia de usuario incoherente en diferentes dispositivos/plataformas

9 % Imposibilidad de conectarse a la VPN o de acceder a las aplicaciones por completo

**Figura 12:** Las quejas más comunes entre los usuarios de VPN.



©2025 Zscaler, Inc. Todos los derechos reservados.

# Gestión de VPN: Sobrecarga de los equipos informáticos y exposición de vulnerabilidades

Las VPN están sobrecargando a los equipos de TI con vulnerabilidades de seguridad persistentes, demandas de mantenimiento que consumen muchos recursos y modelos de acceso obsoletos que ya no se ajustan a las necesidades de los entornos empresariales actuales centrados en la nube. La principal preocupación de estos equipos (52 %) son las brechas de seguridad que provocarán incidentes de seguridad, lo que subraya los riesgos constantes relacionados con el robo de credenciales, los exploits de software sin parchear y los atacantes que aprovechan el acceso a las VPN para realizar movimientos laterales no controlados. Estos riesgos subrayan por qué las VPN se consideran cada vez más como soluciones de acceso con un alto grado de riesgo.

Las VPN se han convertido en una sangría financiera y operativa para los equipos de TI, ya que el 41 % de los encuestados destacan los exorbitantes costos de recursos ligados al mantenimiento de las mismas. El incesante ciclo de aplicación de parches, solución de problemas y supervisión de registros es necesario para asegurar una infraestructura obsoleta, pero deja a los equipos al límite de su capacidad e incapaces de centrarse en actividades de mayor valor.

La incapacidad de las VPN para aplicar controles de acceso granulares es otra debilidad crítica, citada por el 35 % de los encuestados. En lugar de conceder un acceso preciso y basado en la identidad a aplicaciones específicas, las VPN suelen proporcionar una conectividad de red amplia y sin restricciones, lo que aumenta drásticamente el potencial de las amenazas internas y el movimiento lateral de los atacantes. Además, el 26 % menciona la sobrecarga operativa que supone gestionar los concentradores VPN y otros dispositivos, lo que ilustra la complejidad de mantener los aparatos de hardware, los túneles de red y las puertas de acceso para mantener la conectividad remota. Estas complejidades son especialmente insostenibles en una era en la que los entornos de trabajo remotos y nativos de la nube requieren soluciones más ágiles y escalables.

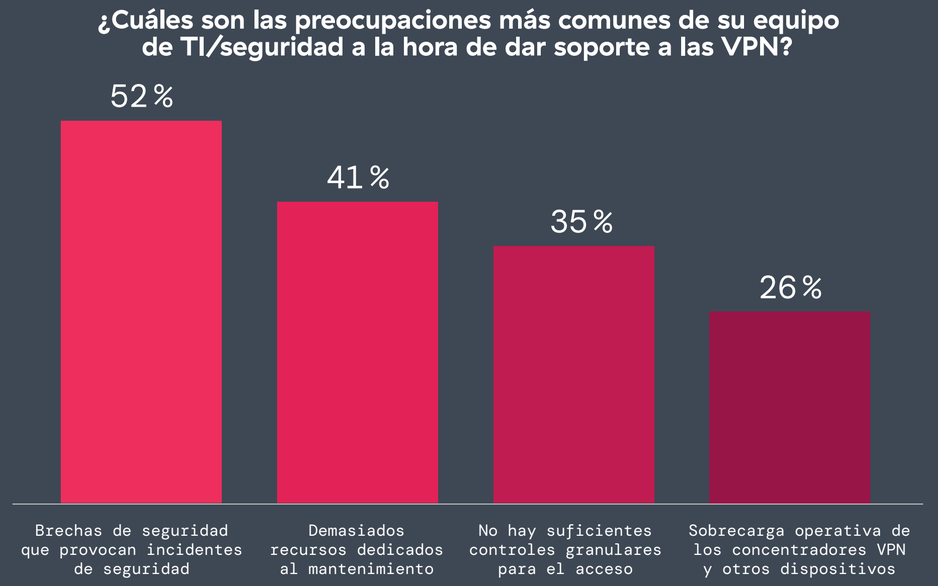



**Figura 13:** Las principales preocupaciones de los equipos de TI y seguridad al dar soporte a las VPN.

**Para hacer frente a estos desafíos, las organizaciones deben pasar de un acceso VPN basado en la red a un modelo Zero Trust en la nube, que elimina la confianza implícita, reduce las superficies de ataque y agiliza las operaciones de TI. La adopción de Zero Trust reduce la sobrecarga operativa relacionada con la VPN, simplifica la gestión del acceso y minimiza los riesgos de seguridad a escala. Los equipos de TI se libran de las tareas de mantenimiento constantes, lo que les permite centrarse en iniciativas de seguridad proactivas y, al mismo tiempo, ofrecer experiencias de usuario más rápidas y fluidas.**


©2025 Zscaler, Inc. Todos los derechos reservados.

# La dura carga de la gestión de VPN

La gestión de la infraestructura VPN sigue sobrecargando a los equipos de TI, y las principales preocupaciones se centran en la confiabilidad, el rendimiento y los gastos generales de mantenimiento. La resolución de problemas de conectividad y estabilidad de las VPN sigue siendo el principal desafío, citado por el 54 % de los encuestados. Los equipos de TI se encuentran en una lucha constante por mantener un tiempo de actividad de las VPN uniforme, con fallas de conexión que crean interrupciones generalizadas que degradan la productividad, comprometen la seguridad y frustran a los empleados.

Equilibrar el rendimiento de las VPN y la experiencia del usuario sigue siendo un desafío importante (50 %), ya que las VPN suelen introducir latencia, desconexiones y velocidades inconsistentes, sobre todo en los entornos en los que prima la nube. Además, el 47 % de los profesionales de TI destacan las frecuentes demandas de aplicación de parches y el costo de los recursos como un obstáculo importante, lo que subraya los desafíos operativos de mitigar las vulnerabilidades persistentes y mantener los sistemas obsoletos.

Estos desafíos han protagonizado varias violaciones de alto perfil. Desde diciembre de 2023 hasta principios de 2024, varias agencias gubernamentales fueron blanco de un ataque relacionado con VPN. Los retrasos en la aplicación de parches a una vulnerabilidad ampliamente conocida permitieron a los actores malintencionados aprovecharse de un software VPN obsoleto, obteniendo acceso no autorizado a la red. Este caso pone de relieve las deficiencias de los ciclos reactivos de aplicación de parches, incluso entre organizaciones con equipos informáticos dedicados, y demuestra cómo unas defensas VPN incompletas exponen a los sectores críticos a amenazas cambiantes.

**Dado que la infraestructura VPN consume importantes recursos de TI para la resolución de problemas de conectividad, la aplicación de parches de seguridad y la optimización del rendimiento, las organizaciones deben reevaluar la viabilidad a largo plazo del acceso basado en VPN. Al sustituir los concentradores VPN y los dispositivos de red como firewalls y NAC por una arquitectura nativa en la nube, los equipos de TI pueden eliminar los cuellos de botella de la infraestructura, reducir los ciclos de aplicación de parches y eliminar la necesidad de solucionar manualmente las fallas de conexión.**

**El acceso con privilegios mínimos basado en políticas garantiza que los usuarios se conecten solo a aplicaciones autorizadas, sin la carga de administrar reglas de firewalls complejas o políticas de segmentación de red. Al realizar la transición a un modelo Zero Trust en la nube, las empresas podrán eliminar los cuellos de botella relacionados con las VPN al tiempo que garantizan un acceso a las aplicaciones sin fisuras y basado en políticas, sin la carga que supone gestionar la infraestructura de red, los parches de software o los complejos esfuerzos de ampliación.**

**¿Cuáles son las tres principales preocupaciones a la hora de gestionar su infraestructura VPN?**

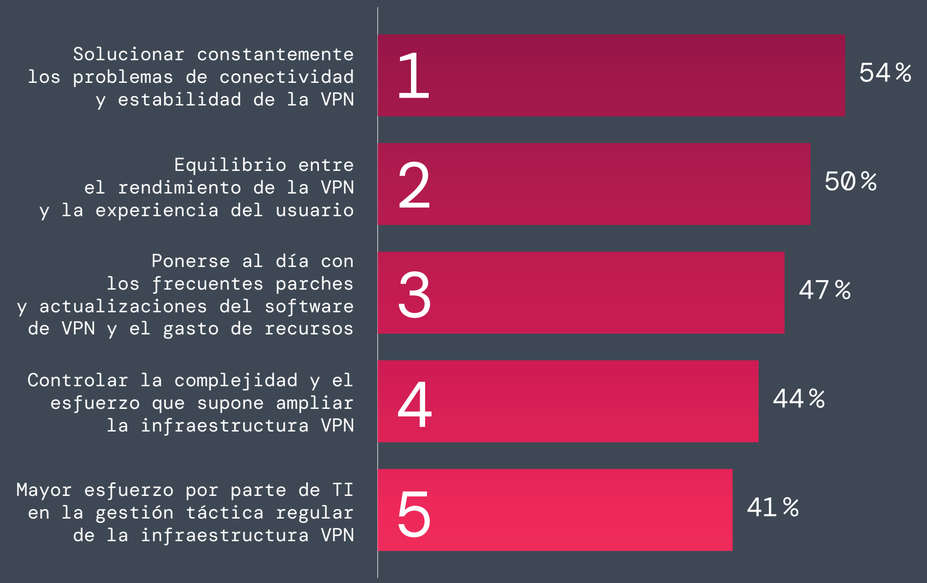



**Figura 14:** Principales preocupaciones de los equipos informáticos que gestionan infraestructuras VPN.


©2025 Zscaler, Inc. Todos los derechos reservados.

# Controles de acceso a VPN demasiado amplios: Una brecha de seguridad crítica

La causa fundamental de muchos riesgos de seguridad de VPN radica en cómo las VPN definen el acceso. En lugar de proporcionar un acceso preciso y específico para cada aplicación, muchas organizaciones siguen concediendo un amplio acceso a la red y se basan en modelos de confianza implícitos, dejando expuestos los sistemas críticos.

Los resultados de las encuestas revelan que el 52 % de las organizaciones aún dependen de modelos de acceso obsoletos, como las reglas estáticas de los firewalls de red (28 %) o el acceso abierto para usuarios autenticados (24 %). Estos controles obsoletos permiten a los atacantes atravesar fácilmente las redes sin ser detectados, escalar privilegios y exfiltrar datos críticos una vez que obtienen el acceso.

Incidentes recientes destacan los peligros de un acceso tan amplio. A principios de 2024, Global Affairs Canada (GAC) experimentó una importante violación de la seguridad debido a una VPN comprometida utilizada por los empleados para acceder a la sede de Ottawa. Los atacantes explotaron las vulnerabilidades de la VPN, obteniendo acceso no autorizado a la red y exponiendo potencialmente información confidencial. El suceso demostró cómo el acceso a la red sin restricciones y con privilegios excesivos proporciona un marco ideal para el movimiento lateral y una infiltración más profunda.

**Para mitigar estos riesgos, las organizaciones deben eliminar la confianza implícita y aplicar controles de acceso granulares y basados en la identidad. Pasar de modelos de acceso amplios basados en la red a una segmentación directa a nivel de aplicación garantiza que un usuario determinado solo pueda acceder a los recursos específicos necesarios para su función, lo que reduce significativamente las superficies de ataque y evita el movimiento lateral.**

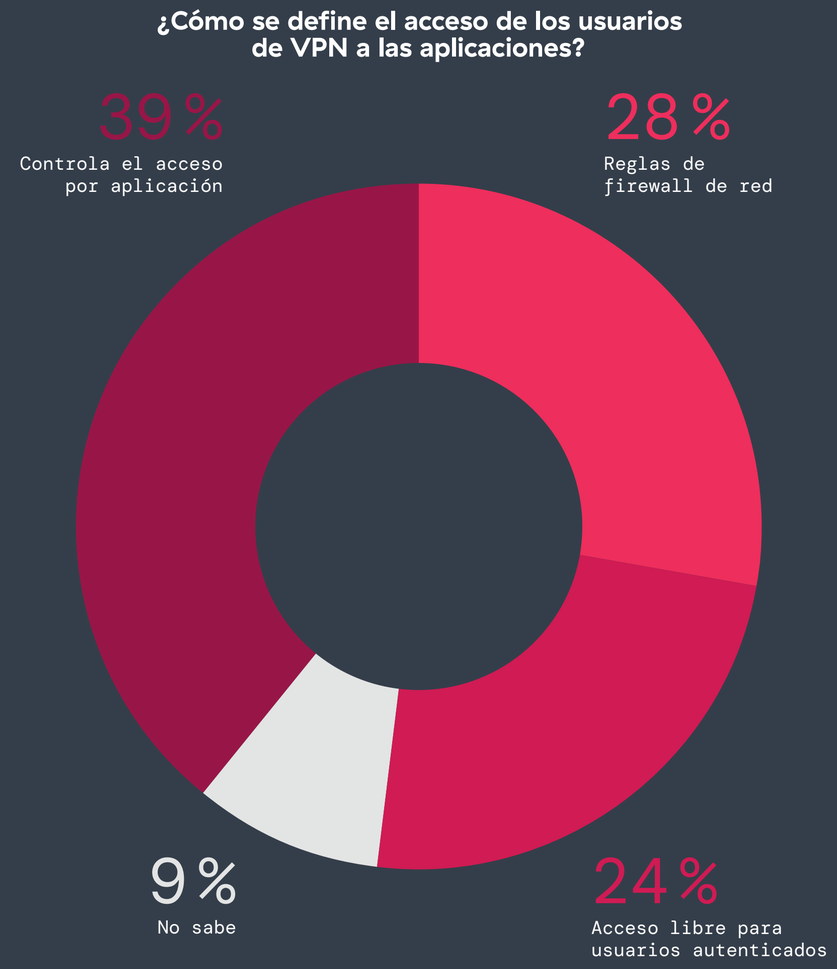



**Figura 15:** Las maneras en que las empresas definen el acceso de los usuarios de VPN alas aplicaciones.


©2025 Zscaler, Inc. Todos los derechos reservados.

# Sustitución de VPN: Un cambio hacia el acceso seguro

Las crecientes vulnerabilidades de seguridad, los desafíos de la experiencia del usuario y la elevada sobrecarga de mantenimiento de las VPN están impulsando a las organizaciones a acelerar su transición a tecnologías modernas de acceso seguro como el ZTNA. Este cambio señala la creciente percepción de que las VPN ya no son capaces de satisfacer las exigencias modernas de seguridad u operativas.

La encuesta confirma este ritmo, ya que el 65 % de los encuestados afirma que sus organizaciones están sustituyendo o planean sustituir sus VPN en el próximo año.

**A medida que las organizaciones se alejan cada vez más de las VPN, deben dar prioridad a la adopción de modelos de seguridad en la nube que impongan un acceso granular a nivel de aplicación en lugar de una amplia conectividad de red. ZTNA elimina los riesgos relacionados con las VPN garantizando que los usuarios solo puedan acceder a los recursos que necesiten, en función de su identidad y su postura de seguridad, sin situarlos nunca en la red corporativa. Este enfoque aumenta la seguridad, reduce la complejidad operativa y mejora la experiencia del usuario, por lo que la sustitución de las VPN es un paso urgente y necesario para las empresas modernas.**

**¿Cuáles son sus planes para reemplazar su servicio VPN actual?**

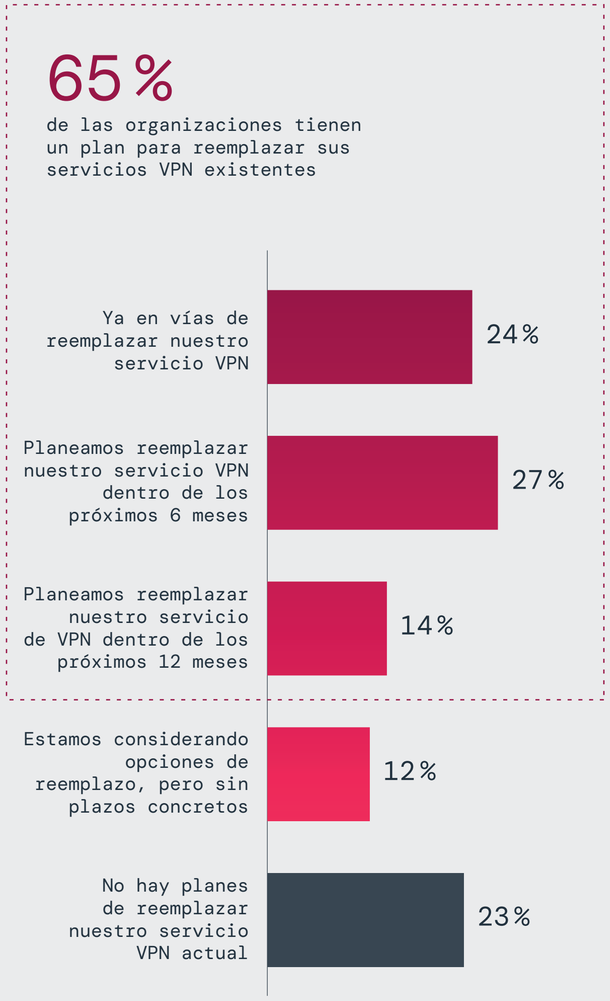
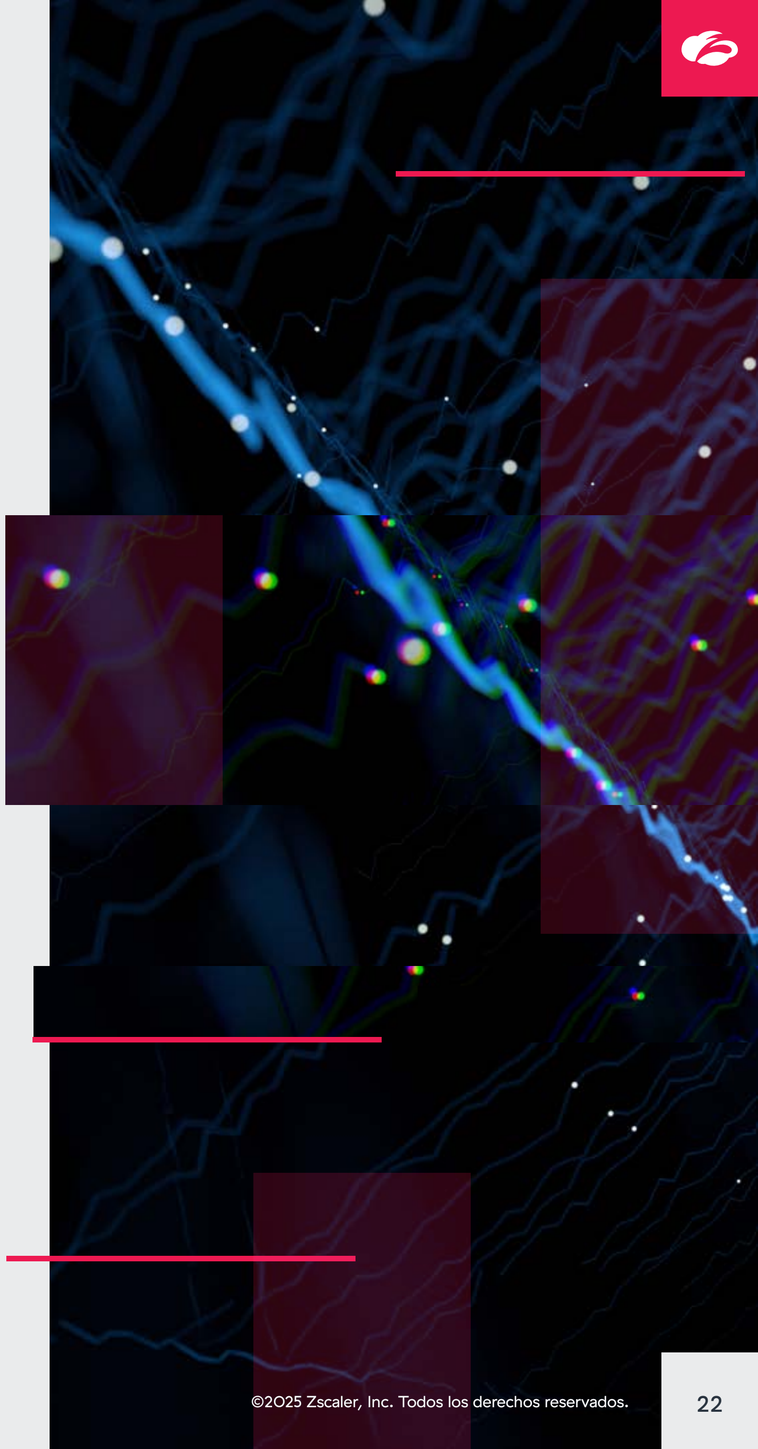



**Figura 16:** Planes empresariales para reemplazar los servicios VPN existentes.




©2025 Zscaler, Inc. Todos los derechos reservados.

# Adopción de Zero Trust

## Zero Trust reemplaza a las VPN a gran escala

A medida que se acelera la tendencia de sustitución de las VPN, la gran mayoría de las organizaciones están recurriendo a arquitecturas Zero Trust para permitir controles de acceso granulares, reducir sus superficies de ataque y mejorar la productividad de los usuarios. Los resultados de la encuesta subrayan la tendencia creciente de este cambio de paradigma: el 81 % de los encuestados indica que tiene previsto adoptar Zero Trust en el plazo de un año. Entre ellos, el 35 % ya está implementando soluciones Zero Trust, el 24 % prevé implementarlas en un plazo de seis meses y el 22 % tiene estrategias de implementación programadas para el año siguiente, lo que demuestra que Zero Trust es la estrategia líder del sector para sustituir a las tecnologías de acceso heredadas, como las VPN.

**Para adoptar Zero Trust con éxito es necesario que los equipos de seguridad y las operaciones empresariales estén alineados. Las organizaciones deben realizar evaluaciones de riesgos para identificar sus puntos de acceso más vulnerables (ya sean accesos remotos, integraciones de terceros o aplicaciones críticas) y priorizar la implementación de Zero Trust como corresponda. El aprovechamiento de la automatización para aplicar las políticas puede acelerar la transición al tiempo que reduce la carga administrativa.**

**¿Qué planes tiene para adoptar una estrategia Zero Trust en su organización?**

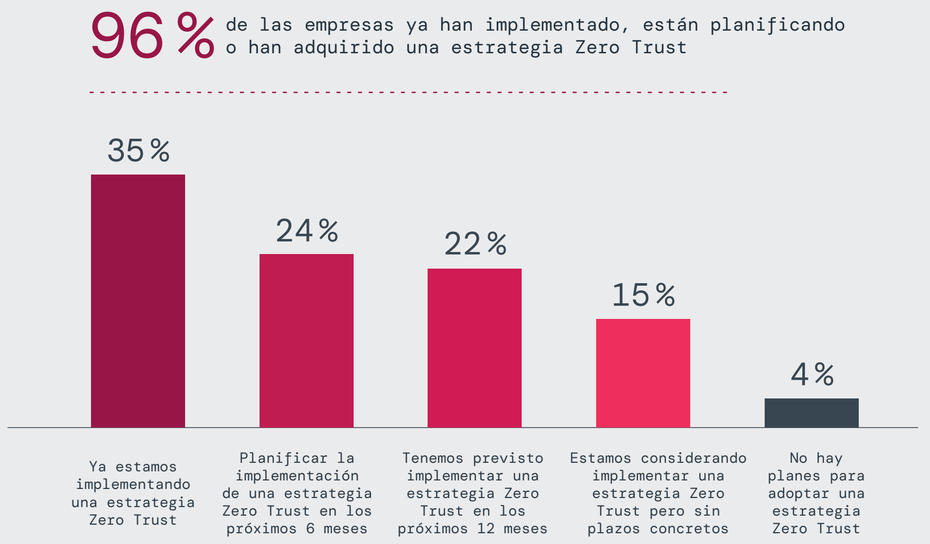



**Figura 17:** Planes empresariales para implementar una estrategia Zero Trust.


©2025 Zscaler, Inc. Todos los derechos reservados.

# Prioridades Zero Trust: el trabajo remoto impulsa la adopción

El alejamiento de las VPN tradicionales subraya una transformación significativa: las organizaciones están recurriendo a arquitecturas Zero Trust para abordar las brechas de seguridad, agilizar las operaciones de TI y satisfacer las demandas de las fuerzas de trabajo remotas descentralizadas. Este giro estratégico destaca Zero Trust como la solución moderna para mitigar los riesgos de las VPN y simplificar la gestión de la seguridad.

Los resultados de la encuesta indican que la seguridad de las fuerzas de trabajo remotas es la principal motivación para este cambio, ya que el 37 % de las organizaciones se centran en el trabajo remoto y el 28 % en la seguridad de las fuerzas de trabajo híbridas. Este cambio refleja una tendencia más generalizada hacia modelos de seguridad que ofrecen un acceso directo y específico a las aplicaciones, reduciendo así las complejidades asociadas a la gestión de múltiples productos puntuales inherentes a las configuraciones de VPN heredadas.

La implementación de un marco Zero Trust no solo refuerza la seguridad, sino que también alivia la carga operativa que supone la gestión de numerosas soluciones de seguridad. Al unificar las políticas y los controles de seguridad en un sistema cohesivo, las organizaciones pueden reducir la carga administrativa y agilizar las operaciones. Por ejemplo, una plataforma Zero Trust que realice múltiples acciones políticas en un único escaneado puede eliminar la necesidad de encadenar varias soluciones, simplificando la experiencia del usuario y manteniendo al mismo tiempo una seguridad sólida.

**Para asegurar eficazmente las plantillas remotas e híbridas con una arquitectura Zero Trust, las organizaciones deben centrarse en integrar medidas de seguridad que minimicen la complejidad. La implementación de una plataforma unificada Zero Trust puede consolidar varias funciones de seguridad, reduciendo la necesidad de múltiples productos puntuales y simplificando la gestión. Este enfoque mejora la seguridad y la eficacia operativa, lo que permite a los equipos de TI centrarse en iniciativas estratégicas en lugar de gestionar una compleja serie de herramientas de seguridad.**

**¿Cuál es el caso de uso principal para implementar una solución Zero Trust?**

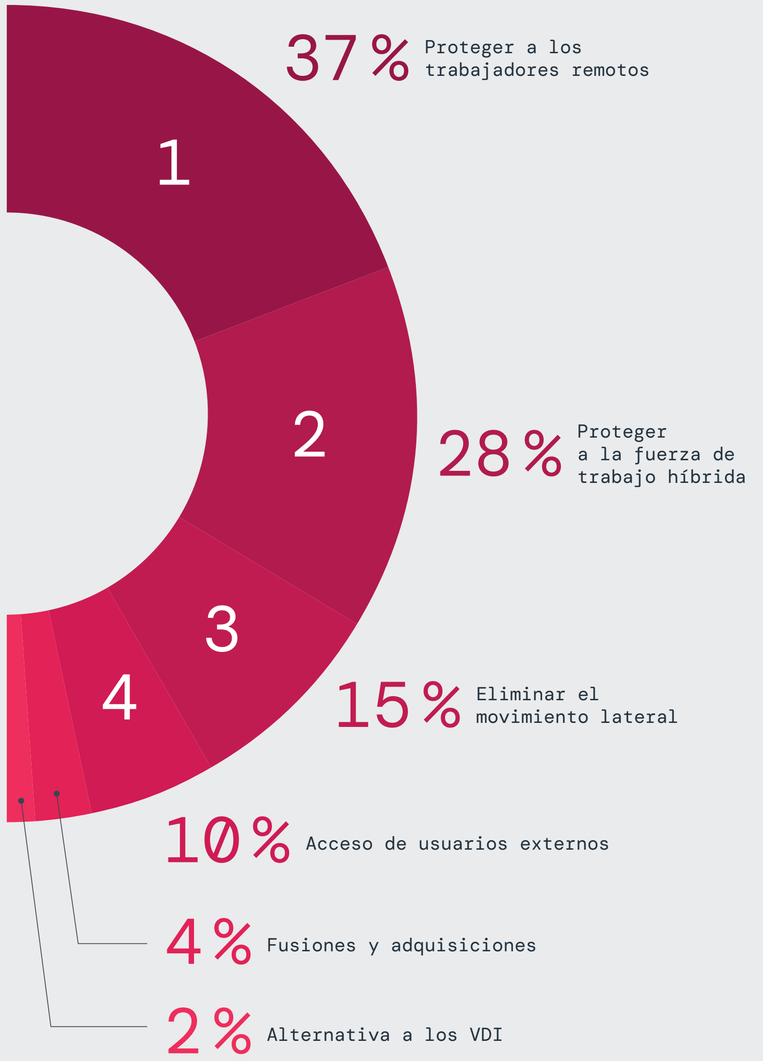



**Figura 18:** Casos de uso principales de las empresas para soluciones Zero Trust.


©2025 Zscaler, Inc. Todos los derechos reservados.

# Principales ventajas de sustituir las VPN por Zero Trust

La adopción de soluciones Zero Trust está transformando la seguridad de las empresas, aportando beneficios de gran alcance que van más allá del acceso seguro, sobre todo en lo que respecta a la simplificación de la gestión, la mejora del rendimiento y la escalabilidad, la reducción drástica de la superficie de ataque y la mejora de la optimización de los recursos. Las organizaciones que sustituyen los modelos VPN por los Zero Trust no están simplemente actualizando las herramientas; están poniendo a prueba de futuro toda su estrategia de acceso remoto.

La gran mayoría de los encuestados (76 %) considera que la mejora de la seguridad y el cumplimiento de las normativas es una ventaja primordial, lo que refuerza cómo Zero Trust sustituye al acceso implícito a la red y reduce la exposición al ransomware, el robo de credenciales y los riesgos de movimiento lateral.

Además, el 64 % señala como ventaja principal las mejoras en la simplicidad de la gestión, la escalabilidad y la experiencia del usuario, ya que Zero Trust elimina las cargas operativas de la gestión de los concentradores VPN, la aplicación constante de parches y la resolución de problemas de acceso.

Cerca de la mitad (45 %) de los encuestados citan la sustitución de la VPN por una solución Zero Trust como un paso crítico hacia una arquitectura Zero Trust completa. Mientras tanto, el 34 % destaca la escalabilidad y flexibilidad superiores que hacen que Zero Trust sea una solución más eficaz para proteger las fuerzas de trabajo remotas e híbridas. Otros beneficios se suman al perfil de valor de Zero Trust: mejora de la experiencia del usuario final (32 %), integraciones sin fisuras en los sistemas informáticos y de seguridad (28 %) y reducción de los costos operativos gracias al ahorro de recursos (18 %). En conjunto, estas ventajas ilustran por qué las organizaciones están abandonando rápidamente las VPN heredadas en favor de Zero Trust.

**ManpowerGroup**, líder mundial en soluciones de mano de obra, presenta un caso práctico contundente para asegurar el acceso con Zero Trust. Ante la tarea de dar soporte a una amplia fuerza de trabajo remota, la organización sustituyó con éxito su infraestructura VPN heredada por una solución Zero Trust de Zscaler. Sorprendentemente, en solo 18 días, ManpowerGroup amplió el acceso seguro a las aplicaciones a más de 30,000 usuarios, consiguiendo una continuidad empresarial ininterrumpida a la vez que reducía drásticamente los tickets del servicio de asistencia en un 97 %. Esta implementación pone de relieve la capacidad de una arquitectura Zero Trust para escalar rápidamente, simplificar las operaciones e impulsar resultados cuantificables para la productividad y la seguridad.

**Si ha sustituido una solución VPN por una Zero Trust, ¿cuáles considera que son las principales ventajas, en comparación con la solución VPN anterior?**

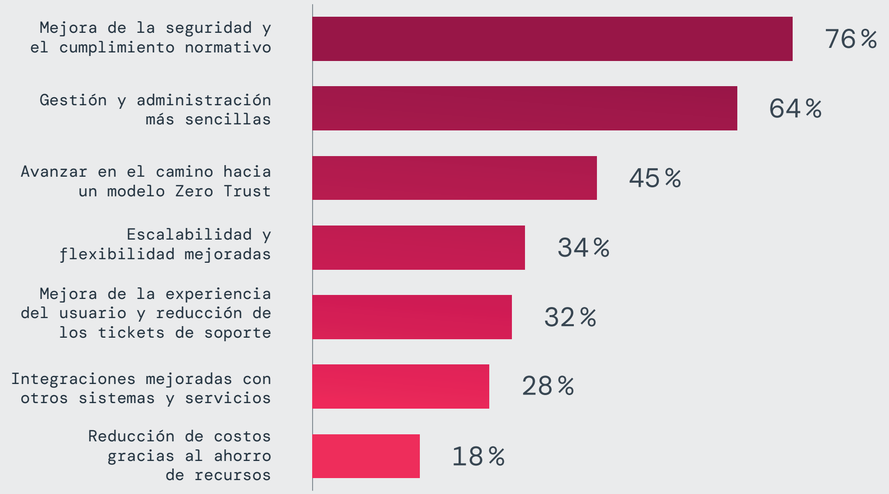



**Figura 19:** Las empresas comparten las principales ventajas de una solución Zero Trust, en comparación con una solución VPN anterior.

**La adopción de Zero Trust debe comenzar con cambios tácticos que eliminen el acceso a la red basado en VPN en favor de conexiones directas a nivel de aplicación para contrarrestar los riesgos de movimiento lateral. Las organizaciones pueden dar prioridad a la sustitución del acceso heredado para casos de uso críticos, como la seguridad de las conexiones de usuarios remotos y de terceros, antes de ampliar las capacidades Zero Trust a todo su ecosistema de TI. La automatización de las políticas de acceso (mediante un único conjunto de políticas) y la integración de la seguridad basada en identidades simplificarán aún más la gestión de Zero Trust al tiempo que permitirán la escalabilidad a través de sistemas distribuidos. Estos marcos inteligentes permiten a los equipos de TI mantener el control de la seguridad en tiempo real sin sacrificar la agilidad ni la eficacia.**


©2025 Zscaler, Inc. Todos los derechos reservados.

# Predicciones de riesgo de VPN para 2025

## Seguirán apareciendo vulnerabilidades críticas en las VPN

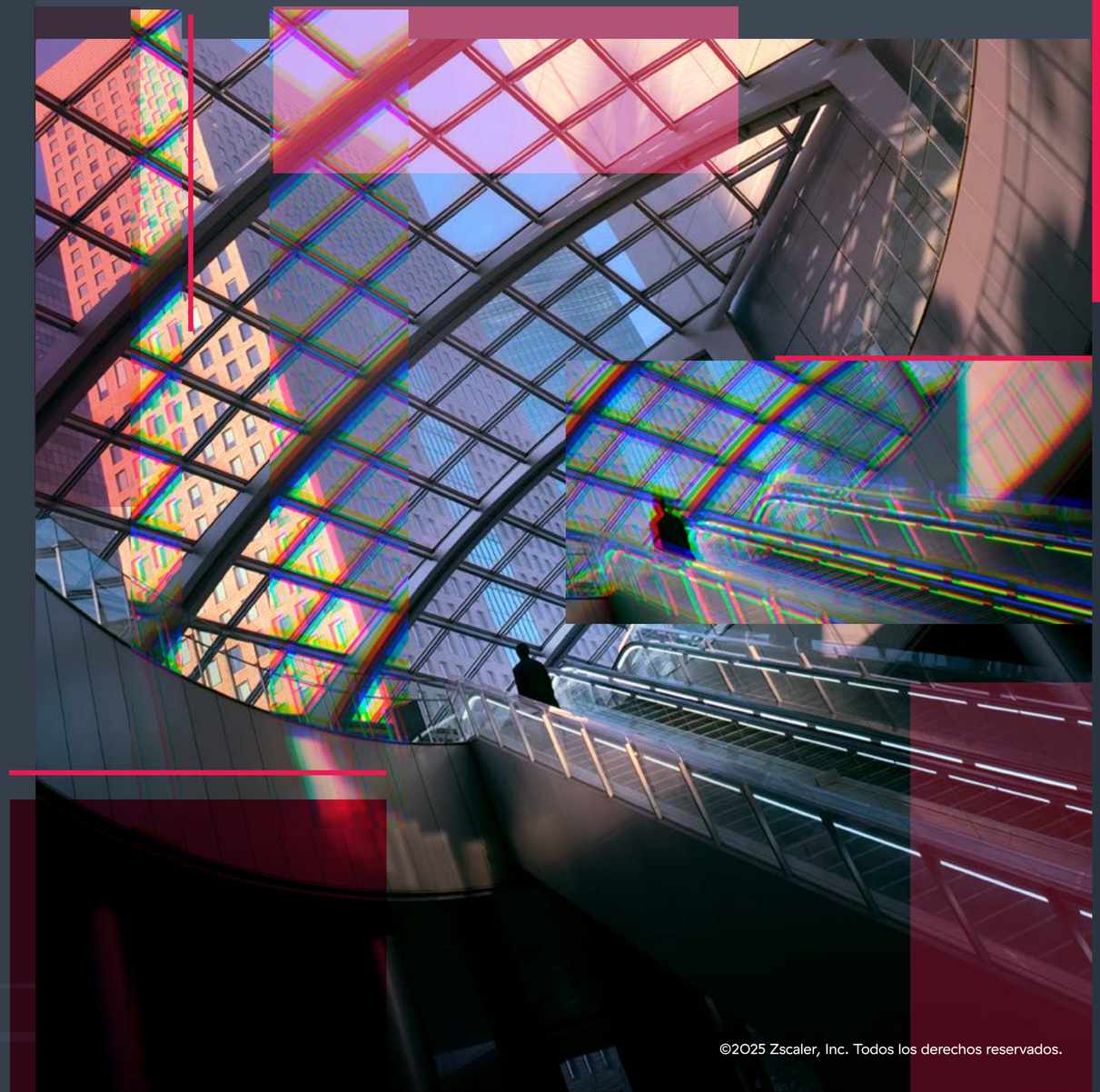
El creciente número de exploits de VPN en los últimos años se acelerará en 2025. Las tecnologías de VPN son un objetivo primordial para los atacantes porque exponen a las empresas a Internet, lo que hace que las vulnerabilidades sean fáciles de escanear y explotar. Mientras las organizaciones se esfuerzan por parchear a tiempo las fallas de las VPN, los atacantes seguirán descubriendo y explotando nuevas vulnerabilidades de alta gravedad, como observamos en la violación de Ivanti Pulse Secure de enero de 2025. Tanto los investigadores de seguridad como los ciberdelincuentes están sondeando activamente las infraestructuras VPN, lo que hace inevitables las continuas revelaciones de CVE críticas.

## Los grupos de ransomware intensificarán los exploits de VPN

Mientras el 92 % de los encuestados expresan su preocupación por las vulnerabilidades de las VPN sin parchear, los actores del ransomware seguirán explotando las fallas conocidas y de día cero de las VPN como método principal de acceso inicial. Los grupos de ransomware como servicio (RaaS) a menudo buscan VPN expuestas con vulnerabilidades sin parchear, lo que les permite implementar ransomware antes de que los equipos de TI puedan responder. La campaña de ransomware de enero de 2025 dirigida a organizaciones sanitarias estadounidenses demuestra cómo las brechas de seguridad de las VPN ofrecen a los atacantes acceso directo a sistemas confidenciales. A medida que estos ataques se vayan automatizando, la necesidad de pasar a una seguridad Zero Trust se volverá aún más urgente.

## El movimiento lateral a través de las VPN impulsará ataques más destructivos

Los atacantes explotan el amplio acceso que proporcionan las VPN para desplazarse lateralmente, escalar privilegios y exfiltrar datos, entre las técnicas más eficaces que utilizan los ciberdelincuentes y los actores de los estados-nación. Dado que el 71 % de las organizaciones están preocupadas por este riesgo, la segmentación de la red suele considerarse una solución, pero su complejidad dificulta su implementación. Muchas organizaciones carecen del personal capacitado para gestionar la segmentación de manera efectiva, lo que da lugar a proyectos que tardan meses en completarse o se estancan por completo. Para mitigar estos desafíos, las empresas deberían adoptar la segmentación Zero Trust, que impone un estricto acceso con privilegios mínimos a las aplicaciones, eliminando las vías de movimiento lateral sin la carga operativa de la segmentación de red tradicional.





©2025 Zscaler, Inc. Todos los derechos reservados.

## El acceso a VPN de terceros seguirá siendo un vector de amenaza clave

Mientras que el 93 % de los encuestados expresan su preocupación por las vulnerabilidades de las VPN de terceros, los atacantes seguirán apuntando a los puntos de acceso externos débiles. Las credenciales de terceros robadas y los accesos VPN mal configurados siguen figurando entre los principales puntos de entrada de los ciberdelincuentes. La violación cometida en 2024 contra el Enterprise Financial Group (EFG) demostró cómo los atacantes aprovechan las conexiones VPN de terceros para infiltrarse en entornos corporativos. Muchas organizaciones carecen de visibilidad sobre los permisos de acceso de terceros, lo que dificulta la aplicación de las políticas de seguridad. Para mitigar estos riesgos, las organizaciones deben hacer la transición a un marco Zero Trust, aplicando un estricto acceso con privilegios mínimos y una verificación continua para todas las conexiones externas.

## Los exploits de VPN impulsados por la IA aumentarán

El auge de los ciberataques impulsados por la IA tendrá un impacto sin precedentes en la seguridad de las VPN. Los atacantes aprovecharán cada vez más la IA para el reconocimiento automatizado, la pulverización inteligente de contraseñas y el rápido desarrollo de exploits, lo que les permitirá comprometer las credenciales de las VPN a escala. Las técnicas de evasión potenciadas por la IA dificultarán aún más la detección de intrusiones basadas en VPN antes de que se produzcan daños significativos. Mientras tanto, las soluciones de seguridad VPN impulsadas por la IA pueden introducir brechas de seguridad imprevistas, dando lugar a nuevos vectores de ataque que los ciberdelincuentes explotarán. A medida que crecen las amenazas impulsadas por la IA, las organizaciones deben adoptar medidas de seguridad proactivas como la verificación continua de la identidad y los controles de acceso Zero Trust.

## Las principales violaciones relacionadas con las VPN serán noticia

Tras las múltiples violaciones de alto perfil que se produjeron en 2024, las organizaciones se enfrentarán a una mayor presión para revelar los ciberincidentes relacionados con las VPN. Con las nuevas normativas de la SEC que exigen transparencia sobre los riesgos de ciberseguridad, las organizaciones que sufran ataques de VPN se enfrentarán a un mayor escrutinio normativo, daños a su reputación y posibles sanciones económicas. A medida que las VPN sigan siendo el principal punto de entrada de los ataques, las organizaciones se verán obligadas a reevaluar los modelos de acceso heredados, acelerando el avance hacia una seguridad Zero Trust.

## Las inversiones en Zero Trust aumentarán a medida que las VPN decaigan

Con un 65 % de las organizaciones que ya han sustituido o tienen previsto sustituir sus VPN en el plazo de un año, la inversión en seguridad Zero Trust se está acelerando, remodelando de manera fundamental el panorama del acceso remoto. Los requisitos normativos y los mandatos de los ciberseguros están impulsando a las organizaciones a ir más allá de las VPN, ya que las soluciones heredadas no consiguen satisfacer las demandas de seguridad, escalabilidad y cumplimiento. La adopción de Zero Trust solo reduce el ciberriesgo, sino que también elimina los elevados costos de mantenimiento de los concentradores VPN, los dispositivos de red y los continuos ciclos de aplicación de parches. Como resultado, las VPN se consideran cada vez más obsoletas, lo que ha provocado un cambio en toda la industria hacia modelos de seguridad Zero Trust.



**Estas predicciones resaltan un consenso creciente: las organizaciones que retrasen la adopción Zero Trust seguirán siendo muy vulnerables a medida que aumenten las vulnerabilidades de VPN. El futuro del acceso seguro depende de la mitigación proactiva de riesgos, no de la aplicación de parches reactivos, por lo que ahora es el momento de ir más allá de las VPN.**


©2025 Zscaler, Inc. Todos los derechos reservados.

# Mejores prácticas para el acceso seguro

## Reducir los riesgos de las VPN y fortalecer la seguridad Zero Trust

1. **Elimine el acceso basado en la red para minimizar la superficie de ataque**
   Evite que los atacantes exploten los puntos de entrada a la red expuestos eliminando gradualmente las VPN y el acceso basado en la red en favor de una conectividad directa y específica de la aplicación. Los datos de la encuesta muestran que el 54 % de las organizaciones citan los riesgos de seguridad como su principal desafío en materia de VPN, lo que refuerza la necesidad de eliminar las dependencias de las VPN y los modelos de seguridad basados en firewalls que exponen a las empresas a los ataques.

2. **Detenga el compromiso inicial con la prevención de amenazas en línea**
   Inspeccione todo el tráfico cifrado y sin cifrar en línea para bloquear los exploits de día cero, el malware y las cargas útiles de ransomware antes de que lleguen a los usuarios. Dado que al 92 % de las organizaciones les preocupa que el ransomware se centre en las vulnerabilidades de las VPN, la inspección del tráfico en tiempo real y el bloqueo basado en políticas son esenciales. Un modelo de seguridad nativo de la nube elimina la necesidad de firewalls locales y reduce la superficie de ataque.

3. **Refuerce la autenticación y la seguridad de la identidad**
   Implemente la autenticación multifactor (MFA) a prueba de phishing, como las credenciales FIDO2, la biometría o los tokens de hardware para verificar el acceso de los usuarios. Evite los métodos de autenticación heredados, como la MFA basada en SMS y las notificaciones push, que los atacantes eluden con frecuencia. Integre la seguridad basada en la identidad con la verificación continua en lugar de confiar en la autenticación única.

4. **Imponga el acceso con privilegios mínimos y basado en el contexto con ZTNA**
   Sustituya el amplio acceso VPN por el acceso a la red Zero Trust (ZTNA) para garantizar que los usuarios solo se conecten a las aplicaciones autorizadas, nunca a la propia red. Los controles de acceso granulares y "just-in-time" (JIT) basados en la identidad, la postura del dispositivo y el análisis de riesgos en tiempo real garantizan que los usuarios solo puedan acceder a lo que necesitan, cuando lo necesitan.

5. **Elimine el movimiento lateral con la segmentación Zero Trust**
   Conecte a los usuarios directamente a las aplicaciones, no a la red, para evitar que los atacantes se desplacen por los sistemas si obtienen el acceso inicial. La segmentación Zero Trust y la microsegmentación consciente de la identidad garantizan que, aunque un usuario se vea comprometido, un atacante no pueda pivotar a otros recursos o escalar privilegios. ZTNA elimina los túneles VPN, que son uno de los principales facilitadores del movimiento lateral.

6. **Asegure el acceso de terceros y externo con controles basados en la identidad**
   Imponga el acceso con privilegios mínimos para terceros, proveedores y contratistas, aplicando estrictos controles de sesión, comprobaciones del estado de los dispositivos y una supervisión continua. Sustituir el acceso de terceros basado en VPN por ZTNA reduce significativamente la exposición al riesgo de credenciales de proveedores comprometidas, un cambio positivo para el 93 % de las organizaciones que se preocupan por los riesgos de las VPN de terceros.




©2025 Zscaler, Inc. Todos los derechos reservados.

7. **Mejore la protección de datos con políticas Zero Trust integradas**
Implemente controles en línea de prevención de pérdida de datos (DLP) y de agente de seguridad de acceso a la nube (CASB) para inspeccionar, cifrar y evitar el movimiento de datos no autorizados en tiempo real. Un marco de seguridad Zero Trust garantiza la inspección y el control de todo el tráfico de usuarios, incluso en aplicaciones SaaS y entornos en la nube.

8. **Implemente la seguridad impulsada por la IA y la supervisión continua**
Utilice la analítica impulsada por la IA en tiempo real, la tecnología del engaño y la detección automatizada de comportamientos para detener las amenazas antes de que se intensifiquen. Las soluciones ZTNA proporcionan una puntuación de riesgos en tiempo real, impidiendo que las cuentas comprometidas accedan a aplicaciones confidenciales. La caza proactiva diaria de amenazas y los controles de acceso basados en el riesgo reducen significativamente el impacto de las violaciones.

9. **Evalúe y adapte continuamente la postura de seguridad**
Realice evaluaciones de riesgos automatizadas, pruebas de penetración y simulaciones de adversarios para ajustar dinámicamente las políticas de seguridad Zero Trust. Los errores de configuración de la seguridad y la no aplicación de las políticas contribuyen en gran medida a las violaciones importantes, por lo que la aplicación automatizada de las políticas es fundamental para reducir los errores humanos.

10. **Elimine la infraestructura VPN y automatice la aplicación de las políticas de seguridad**
Elimine la necesidad de concentradores VPN, gestión de reglas de firewalls y listas de control de acceso manuales adoptando un modelo Zero Trust en la nube. El ZTNA permite políticas de seguridad dinámicas que se adaptan en tiempo real a los cambios de cumplimiento, las actualizaciones normativas y las ciberamenazas en evolución, sin necesidad de configuración manual ni dependencias de hardware.

Mediante la aplicación de estas mejores prácticas, las organizaciones pueden eliminar los riesgos de seguridad de las VPN con un marco de seguridad Zero Trust resiliente, que garantice la verificación continua, el acceso con privilegios mínimos y la mitigación proactiva de las amenazas.




©2025 Zscaler, Inc. Todos los derechos reservados.

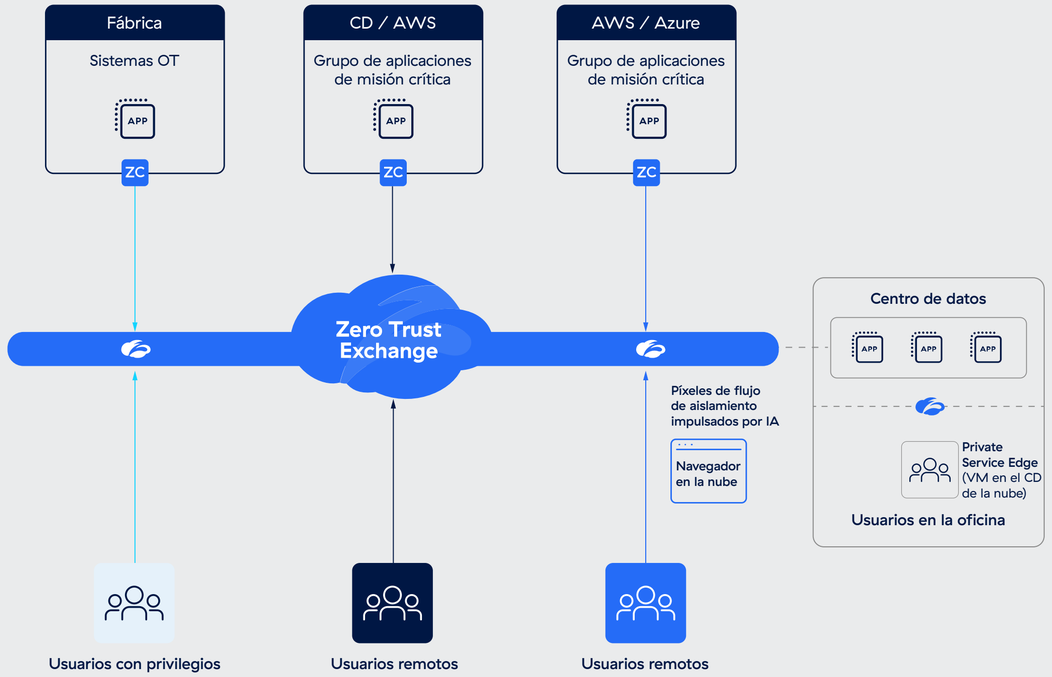
# Cómo Zscaler transforma el acceso seguro

Las VPN y los firewalls tradicionales amplían significativamente la superficie de ataque de una organización al colocar a los usuarios directamente en la red. Este amplio acceso facilita a los atacantes explotar las vulnerabilidades, entrar y desplazarse lateralmente dentro del entorno. A medida que las amenazas continúan evolucionando y el trabajo híbrido se convierte en la norma, confiar en estas tecnologías obsoletas plantea riesgos de seguridad críticos que exigen soluciones más seguras y adaptables.

Zscaler Private Access™ (ZPA) proporciona una alternativa segura y escalable a las soluciones de acceso remoto heredadas como las VPN. Como solución nativa de la nube, ZPA permite el acceso Zero Trust para todos los usuarios ofreciendo conectividad directa a aplicaciones privadas. Para minimizar la superficie de ataque, las aplicaciones están protegidas detrás de la plataforma Zscaler Zero Trust Exchange™. Este enfoque elimina el movimiento lateral a través de la segmentación de usuario a aplicación impulsada por la IA y defiende contra amenazas sofisticadas con inspección de tráfico integrada, así como protección de aplicaciones y datos.

ZPA se puede implementar en cuestión de horas para reemplazar las VPN heredadas y las herramientas de acceso remoto con una plataforma integral Zero Trust. Impulsado por la nube de seguridad más grande del mundo, ZPA ofrece conectividad rápida, confiable y de baja latencia a usuarios en cualquier parte del mundo. Su arquitectura nativa de la nube garantiza una escalabilidad elástica y satisface sin problemas las necesidades de las fuerzas de trabajo distribuidas e híbridas en distintas ubicaciones geográficas.

Con ZPA, las empresas pueden adoptar y centrados en la nube con confianza, sabiendo que sus recursos están protegidos, sus usuarios son productivos y sus operaciones de TI están preparadas para el futuro.






©2025 Zscaler, Inc. Todos los derechos reservados.



# Principales ventajas de Zscaler Private Access (ZPA)

## Minimice la superficie de ataque para protegerse contra ataques de ransomware

Las vulnerabilidades de las VPN exponen a las organizaciones a usuarios malintencionados, lo que provoca ataques de ransomware y robo de credenciales. ZPA elimina este riesgo ocultando todas las aplicaciones detrás Zero Trust Exchange y otorgando a los usuarios acceso directo y Zero Trust solo a las aplicaciones autorizadas. Al impedir que los usuarios no autorizados, incluidos los proveedores y contratistas externos, descubran las aplicaciones y se desplacen lateralmente, la ZPA protege eficazmente contra los ataques de ransomware. Permite el acceso remoto seguro para todas las aplicaciones, incluidas aplicaciones privadas, aplicaciones conectadas a la red como VoIP y aplicaciones de servidor a cliente. Además, ZPA minimiza el impacto de las interrupciones a través de una solución integral de continuidad empresarial y ayuda a las organizaciones a cumplir estrictos requisitos de cumplimiento.

## Eliminación del movimiento lateral de amenazas

ZPA aplica el acceso con privilegios mínimos conectando a los usuarios directamente a aplicaciones específicas, impidiendo el acceso a otras aplicaciones de la red. Proporciona información visual sobre el acceso de usuario a aplicación y las políticas aplicadas, mejorando la visibilidad y el control.

ZPA AI–Powered Segmentation genera automá–ticamente recomendaciones para segmentos de aplicaciones y políticas, simplificando la implementación de la segmentación al tiempo que garantiza la escalabilidad y una seguridad robusta.

## Obtenga visibilidad y análisis granulares

ZPA proporciona visibilidad detallada y en tiempo real del uso de las aplicaciones, el comportamiento de los usuarios y los patrones de acceso. Los equipos de TI pueden usar estos datos para supervisar, auditar e identificar rápidamente posibles amenazas, mejorando así la seguridad general. Esto también puede contribuir al cumplimiento normativo.

## Ofrezca acceso sin clientes para mitigar las vulnerabilidades de terceros

ZPA Clientless Access simplifica el acceso de terceros permitiendo a los contratistas y socios conectarse de manera segura a las aplicaciones a través de cualquier navegador sin necesidad de un cliente. Aísla los dispositivos no gestionados de la red corporativa, protege los datos confidenciales y se integra con Google Chrome Enterprise Browser para mejorar la seguridad BYOD. Este moderno enfoque reduce los costos, minimiza los riesgos asociados al acceso de terceros y elimina la dependencia de la gestión de VDI heredada.


©2025 Zscaler, Inc. Todos los derechos reservados.

## Prevenga el compromiso de aplicaciones privadas

ZPA minimiza el riesgo de compromiso de las aplicaciones privadas y la pérdida de datos al realizar una inspección completa en línea del tráfico de las aplicaciones privadas de extremo a extremo. Las sólidas funciones de prevención de pérdida de datos garantizan que la información confidencial permanezca segura a la vez que bloquean el acceso no autorizado. Al ocultar las aplicaciones de la red de Internet pública y permitir conexiones seguras de usuario a aplicación basadas en principios Zero Trust, la ZPA reduce la superficie de ataque, impide el movimiento lateral y protege contra las violaciones, mejorando la seguridad general.

## Simplifique la gestión de políticas y acelere la implementación

ZPA agiliza las operaciones de TI simplificando la implementación del acceso remoto, la gestión de políticas y la segmentación de usuario a aplicación. Tareas que antes llevaban mucho tiempo, como la incorporación de usuarios, la aplicación de parches y las actualizaciones, ahora pueden completarse en cuestión de minutos, lo que reduce significativamente el esfuerzo de TI. Con una gestión centralizada y recomendaciones de políticas automatizadas, ZPA permite a los equipos de TI mejorar la eficiencia, minimizar la complejidad y centrarse en iniciativas estratégicas en lugar de en las operaciones diarias.

## Aplique el control de acceso basado en la postura

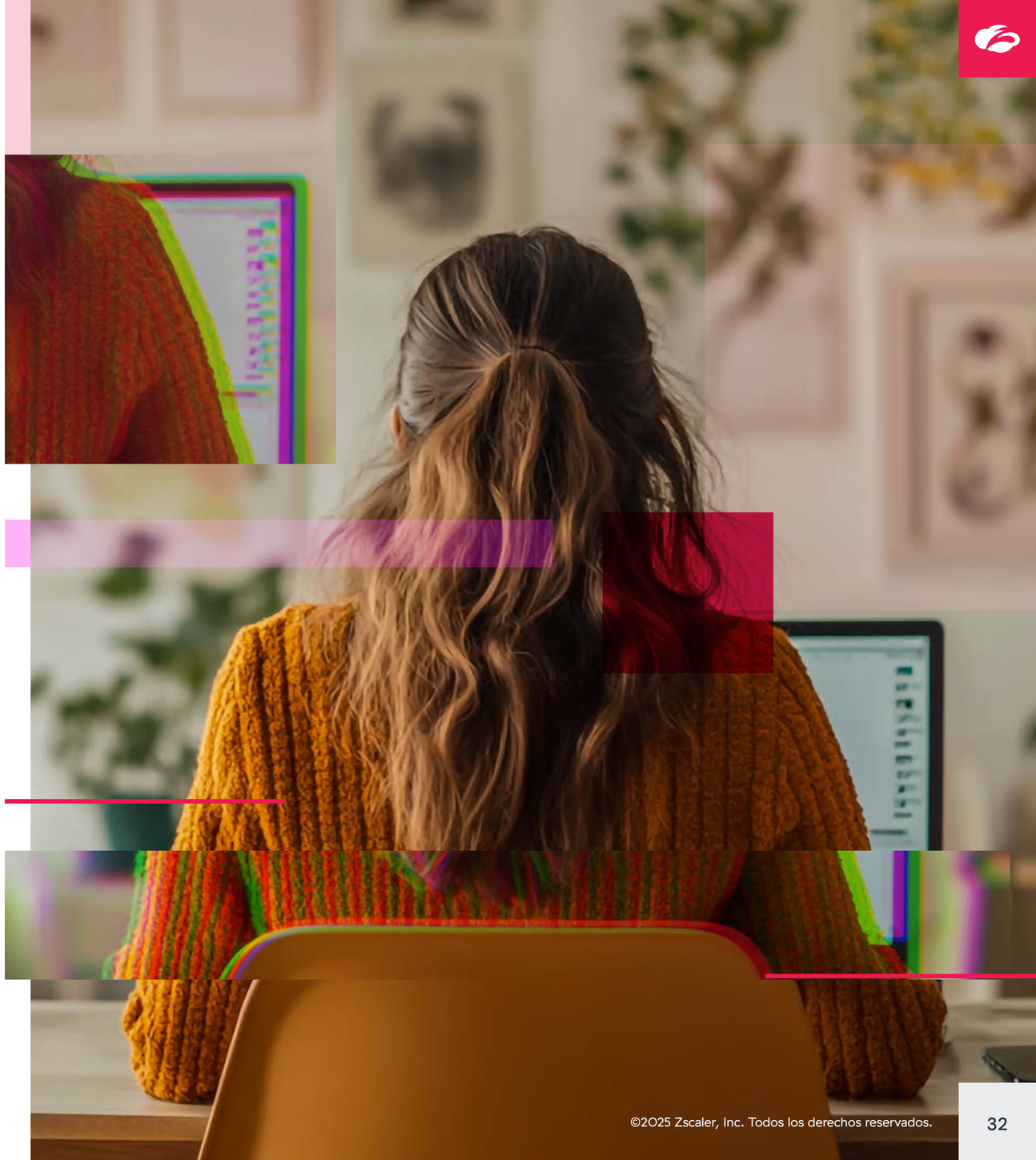
ZPA se integra con herramientas de evaluación de la postura de los puntos finales para verificar la postura de seguridad de los dispositivos del usuario antes de otorgar acceso. Esto garantiza que solo los dispositivos compatibles puedan conectarse, lo que mitiga los riesgos de dispositivos no administrados o comprometidos.

## Ofrezca experiencias de usuario superiores

ZPA garantiza experiencias de usuario óptimas al brindar conectividad rápida, fluida y segura a aplicaciones críticas para la empresa. A diferencia de las VPN que reenvían el tráfico a través de un centro de datos centralizado, la ZPA permite las conexiones directas entre usuarios y aplicaciones a través Zero Trust Exchange. Esto reduce drásticamente la latencia y mejora el rendimiento de la aplicación, ya sea que los usuarios estén en el sitio, de nmanera remota o en movimiento. Al minimizar los inicios de sesión múltiples y la dependencia del software basado en el cliente, ZPA simplifica el acceso y aumenta la productividad. Además, las capacidades de supervisión proactivo de ZPA agilizan la resolución de problemas, garantizando un acceso ininterrumpido y de alta calidad para todos los usuarios.

## Reduzca el costo total de propiedad

ZPA reduce significativamente el costo total de propiedad al eliminar la necesidad de múltiples productos puntuales, como VPN, firewalls, NAC y concentradores VPN. Construido sobre una arquitectura Zero Trust nativa de la nube, ZPA elimina los costos de infraestructura relacionados con el soporte de hardware, el mantenimiento, las reparaciones y las actualizaciones. Su gestión simplificada y la aplicación automatizada de políticas reducen la sobrecarga operativa, lo que permite a los equipos de TI ahorrar tiempo y recursos al tiempo que mejoran la seguridad y la escalabilidad.





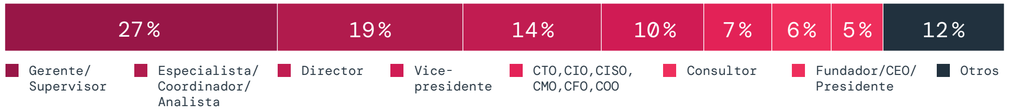
©2025 Zscaler, Inc. Todos los derechos reservados.



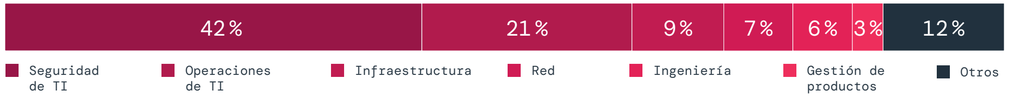
# Metodología_y demografía

Este informe se basa en una encuesta exhaustiva realizada a 632 profesionales de TI y ciberseguridad a principios de 2025, en la que se examinan los riesgos de seguridad de las VPN, las tendencias de acceso de las empresas y la adopción de arquitecturas Zero Trust. Entre los encuestados se encontraban ejecutivos, profesionales de seguridad informática y líderes de infraestructura de red de diversas industrias. Las conclusiones de este informe proporcionan una perspectiva basada en datos sobre el declive de las VPN y el cambio a Zero Trust, ofreciendo una visión crítica para las organizaciones que modernizan sus estrategias de seguridad de acceso.

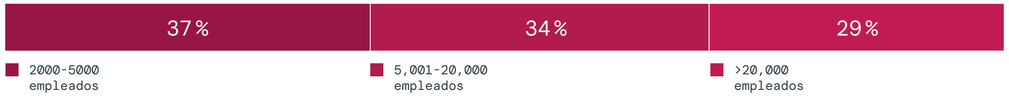
### Nivel de carrera profesional



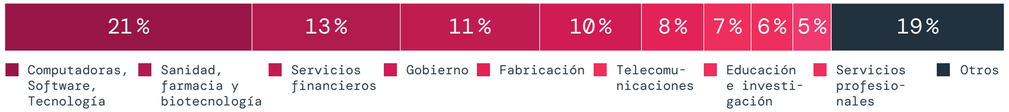

### Departamento




### Tamaño de la empresa




### Sector



# Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zero Trust Exchange™ protege a miles de clientes contra ciberataques y pérdida de datos al conectar usuarios, dispositivos y aplicaciones de manera segura en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange, basado en SASE, es la plataforma de seguridad en la nube en línea más grande del mundo. Para obtener más información, visite **www.zscaler.com/mx.**

# Acerca de ThreatLabZ

ThreatLabz es la rama de investigación de seguridad de Zscaler. Este equipo de primer nivel es responsable de la búsqueda de nuevas amenazas y de garantizar que las miles de organizaciones que utilizan la plataforma global de Zscaler estén siempre protegidas. Además de la investigación de malware y el análisis conductual, los miembros del equipo están involucrados en la investigación y el desarrollo de nuevos módulos de prototipo para la protección avanzada contra amenazas en la plataforma Zscaler, y realizan auditorías de seguridad internas regularmente para garantizar que los productos e infraestructura de Zscaler cumplan con los estándares de seguridad. ThreatLabz publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal, **research.zscaler.com**.



# Acerca de Cybersecurity Insiders

**CYBERSECURITY INSIDERS: SU FUENTE DE CONFIANZA PARA OBTENER INFORMACIÓN SOBRE CIBERSEGURIDAD BASADA EN DATOS**

Cybersecurity Insiders ofrece perspectivas respaldadas por pruebas y validaciones de terceros, lo que permite a los líderes en ciberseguridad tomar decisiones estratégicas con conocimiento de causa. Basándonos en más de una década de investigación con una red global de más de 600,000 profesionales de la ciberseguridad, ofrecemos inteligencia procesable que ayuda a los líderes a afrontar las amenazas en evolución, evaluar las nuevas tecnologías y dar forma a estrategias de futuro con confianza.

Para los proveedores de ciberseguridad, convertimos los resultados de la investigación en resultados: generamos credibilidad, visibilidad y confianza a través de formatos de gran impacto, como informes de mercado y seminarios web basados en datos que establecen un liderazgo de pensamiento, guías de CISO que muestran las mejores prácticas, revisiones de productos que validan soluciones, artículos prácticos que educan a los compradores y reconocimiento mediante premios que elevan la reputación de la marca.

Al combinar este contenido con una distribución integrada, ayudamos a las marcas a ganarse la confianza, amplificar la concientización e impulsar la demanda en el mercado saturado de la ciberseguridad.

Más información: cybersecurity-insiders.com



**Holger Schulze**
CEO y fundador de
Cybersecurity Insiders

©2025 Zscaler, Inc. Todos los derechos reservados.



zscaler™ | Zero Trust Everywhere

## Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales listadas en **zscaler.com/mx/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca comercial es propiedad de sus respectivos propietarios.

**+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134 zscaler.com/mx**

