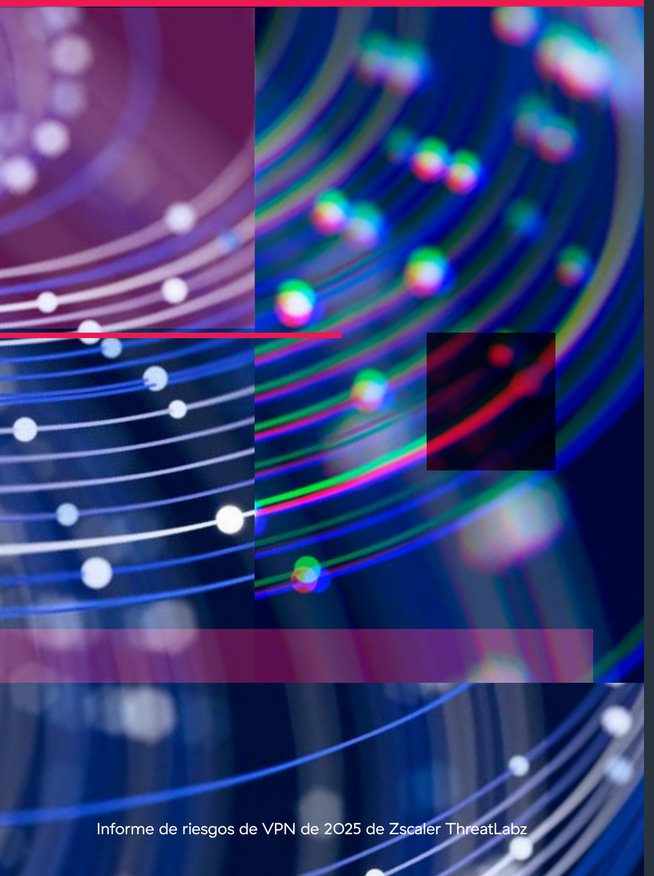
Cybersecurity INSIDERS

Zscaler Informe de riesgos de las VPN de ThreatLabz 2025

Índice



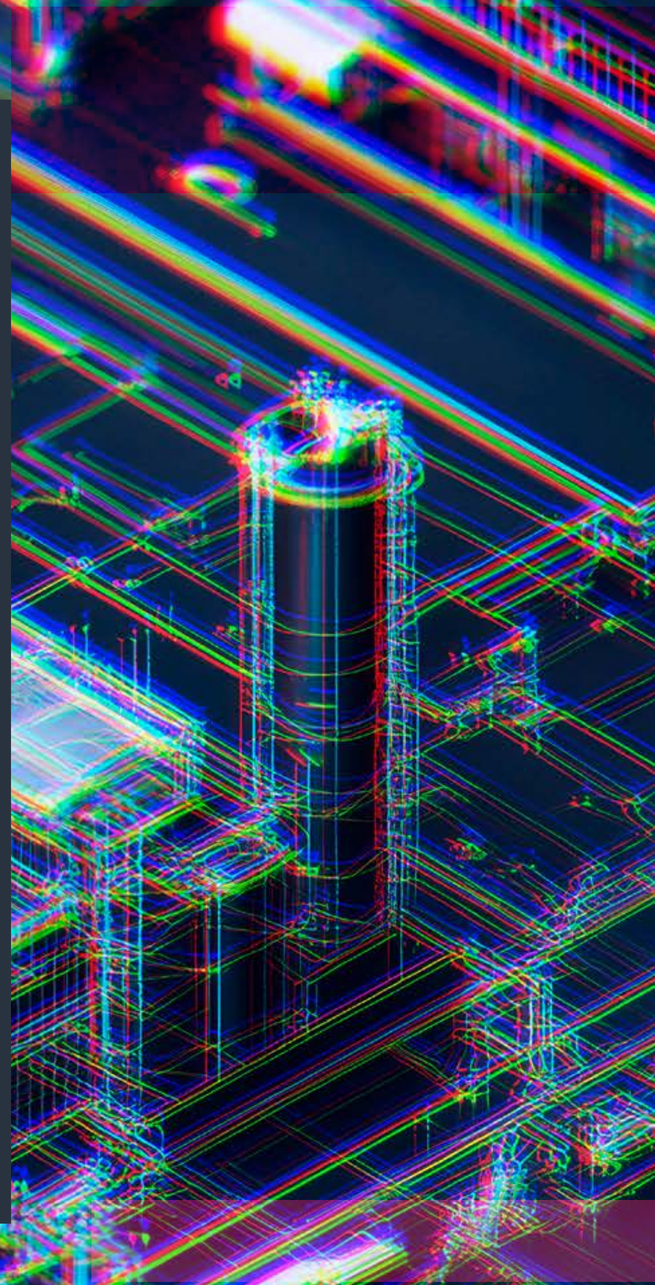
Resumen ejecutivo

El Informe de Riesgos de las VPN 2025 de Zscaler ThreatLabz ofrece una visión profunda de los riesgos en constante evolución asociados a las redes privadas virtuales (VPN) y subraya la urgente transición hacia arquitecturas de zero trust a medida que las organizaciones se esfuerzan por satisfacer las demandas de seguridad a prueba de futuro. Consideradas antaño 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 representar importantes riesgos de seguridad para organizaciones de todo el mundo. Este informe, basado en las opiniones de más de 600 profesionales de TI y seguridad, revela un cambio crucial en el panorama de la ciberseguridad: **más de la mitad de las organizaciones encuestadas sufrieron ataques debido a vulnerabilidades de VPN solo el año pasado,** lo que pone de relieve la urgente necesidad de un nuevo enfoque en los entornos de trabajo cada vez más híbridos de la actualidad.

En 2025, el descontento con las VPN tradicionales ha impulsado un cambio, y las empresas reconocen de forma abrumadora que corregir estas vulnerabilidades es una carrera que ya no pueden ganar. Esto impulsa la adopción generalizada de modelos de 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 de zero trust para 2026 y el 65 % planea eliminar por completo las VPN en dicho 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 de zero trust que garanticen un acceso fluido y seguro.

Entretanto, todos estos cambios se producen en el contexto de un panorama de amenazas impulsado por la IA. De hecho, el aumento de los ciberataques impulsados por IA afectará la seguridad de las VPN de maneras sin precedentes. Los atacantes utilizarán cada vez más la IA para el reconocimiento automatizado de las vulnerabilidades de las VPN, que se analizan fácilmente a través de Internet público. Técnicas como la pulverización inteligente de contraseñas y el desarrollo rápido de exploits permitirán a los ciberdelincuentes comprometer las credenciales de VPN a mayor escala. Más abajo en la cadena de ataque, las técnicas de evasión impulsadas por IA harán que sea aún más difícil detectar intrusiones basadas en VPN antes de que se produzcan daños significativos. A medida que aumentan las amenazas impulsadas por la IA, los riesgos de las VPN sólo se magnificarán, lo que impulsará a las empresas a adoptar medidas de seguridad proactivas y acelerará el cambio ya pronunciado hacia soluciones de zero trust.

Reconociendo estos cambios, el informe de ThreatLabz no sólo traza el declive de las VPN que pasan de ser herramientas indispensables a convertirse en un lastre, sino que también brinda información útil para las empresas que navegan por este panorama transformador.



Principales_ conclusiones

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

   Se espera que un significativo 65 % de las empresas reemplacen sus servicios de VPN durante el próximo año, lo que supone un aumento del 23 % con respecto a 2024. Esta tendencia se debe principalmente a la incapacidad de las VPN de satisfacer las demandas 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. **Aumento de los ciberataques explotados mediante VPN y preocupaciones sobre ransomware:**

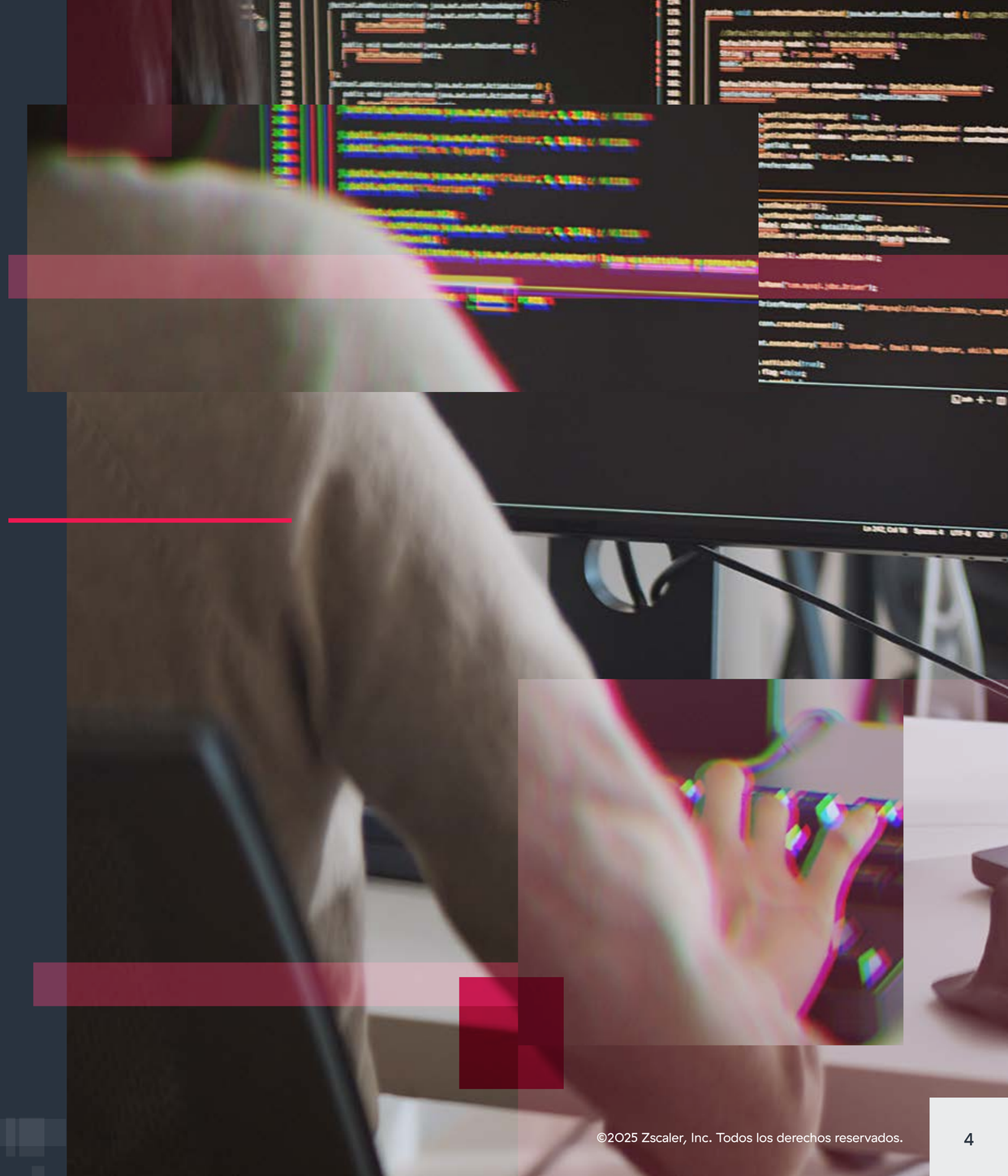
   El año pasado se observó un aumento preocupante en los incidentes cibernéticos relacionados con vulnerabilidades de VPN: el 56 % de las organizaciones informaron de dichas infracciones, un aumento alarmante respecto de las cifras anteriores. Mientras tanto, el 92 % de los encuestados se muestra preocupado de que las vulnerabilidades de VPN sin revisar conduzcan directamente a ataques de ransomware. Estos hallazgos respaldan la tendencia de que, en su esfuerzo por mantener el rápido ritmo de revisión de vulnerabilidades, las empresas necesitan una revisión de seguridad potente para llenar estas brechas de seguridad críticas y mitigar los riesgos siempre presentes de explotación de VPN.

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

   Las frustraciones de los usuarios por las ineficiencias de las VPN (que van desde velocidades lentas hasta una autenticación engorrosa, compleja o defectuosa) influyen cada vez más en las estrategias de las organizaciones. Este descontento del usuario final está impulsando el avance hacia arquitecturas de zero trust que ofrecen acceso seguro e ininterrumpido sin los problemas tradicionales asociados con las VPN.

4. **La transición de la VPN a la zero trust: del concepto a la implementación:**

   Como reflejo de un cambio estratégico importante, el 81 % de las organizaciones avanzarán activamente hacia la implementación de marcos de zero trust durante el próximo año. Esto marca una transición fundamental desde considerar la zero trust como un ideal teórico a reconocerla como una necesidad práctica para reemplazar las VPN y, al mismo tiempo, mejorar la seguridad en entornos de TI dinámicos y distribuidos.



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 con ellos los atacantes. Hoy en día, las VPN suelen servir como puntos de entrada para ataques de ransomware, robo de credenciales y ciberespionaje debido a vulnerabilidades difíciles de revisar rápidamente, modelos de confianza implícita que proporcionan acceso completo a la red y permisos de acceso generalizados. En resumen, las vulnerabilidades de seguridad son el mayor desafío al que se enfrentan las empresas con las VPN (según el 54 % de los encuestados), lo que subraya que los atacantes explotan habitualmente fallos sin revisar o eluden las protecciones para infiltrarse en las redes.

Los riesgos se acentúan aún más con el acceso a VPN de terceros. Un impresionante 93 % de los encuestados expresa su preocupación por las vulnerabilidades de puerta trasera introducidas por las conexiones VPN externas, ya que los atacantes explotan cada vez más las credenciales de terceros para vulnerar las redes sin ser detectados. No se trata únicamente del acceso inicial: las VPN también hacen que las vulneraciones sean más destructivas. A diferencia de las soluciones de 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 identifica el movimiento lateral como una de las principales preocupaciones, reconociendo cómo amplifica el alcance y el impacto de una vulneración.

Estos desafíos, sumados a preocupaciones cotidianas como rendimiento lento, autenticación compleja y desconexiones frecuentes, dejan claro por qué las empresas están abandonando las VPN en favor de modelos de zero trust. El Informe de Riesgos de las VPN 2025, basado en información suministrada por 632 profesionales de TI y ciberseguridad, tiene como objetivo arrojar luz sobre el estado del uso de VPN en 2025 para comprender mejor los riesgos y desafíos, además de ofrecer a las empresas una guía de mejores prácticas para mejorar su postura de ciberseguridad y su enfoque para proteger el acceso remoto.

Los hallazgos de este informe ofrecen a los líderes de TI y seguridad información basada en datos sobre las razones para retirar las VPN obsoletas y adoptar una arquitectura de zero trust moderna basada en la nube. El cambio de la confianza implícita a la verificación continua ya no es opcional: es esencial para proteger a las empresas distribuidas actuales, reducir la complejidad de TI y garantizar una experiencia de usuario fluida.

Preocupaciones de seguridad de las VPN

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

Eliminar las dependencias de VPN ya no es una actualización opcional: es una necesidad inmediata. Las organizaciones necesitan realizar la transición a verdaderos marcos zero trust que ofrezcan acceso con privilegios mínimos basado en la identidad y segmentación granular. Estas arquitecturas distribuidas en la nube ayudan a reducir las superficies de ataque laterales, mejorar las experiencias de los usuarios y disminuir la complejidad de TI: una trilogía de ventajas que las VPN simplemente no pueden igualar.

Las organizaciones que siguen dependiendo de 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 sentimiento creciente de que las VPN pertenecen a una era pasada de la seguridad del acceso.

El principal desafío, 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 a las VPN como puntos débiles propicios para la explotación, mientras que las organizaciones luchan por revisar estos sistemas obsoletos con la suficiente rapidez para mantenerse al día con las amenazas avanzadas.

La frustración de los usuarios ha llegado a un punto crítico: el 51 % de los encuestados identifica el bajo rendimiento de la VPN (incluidos elementos como conectividad lenta, interrupciones y protocolos de autenticación engorrosos) como un obstáculo para la productividad. Las VPN siguen siendo una carga operativa: el 41 % de los encuestados menciona dificultades en la gestión y el 37 % señala los altos costes del mantenimiento continuo. Estas cifras ilustran cómo las VPN se han vuelto consumidoras de muchos recursos, agotando los presupuestos de TI y obligando a los equipos a dedicar tiempo innecesario en tareas repetitivas de resolución de problemas.

Adiós a los enfoques heredados, bienvenido el modelo de zero trust

Una infracción reciente sirve como crudo 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, otorgando acceso no autorizado a través de redes corporativas. Este ataque, uno de varios contra la tecnología VPN en los últimos meses, resalta por qué las organizaciones ya no pueden darse el lujo de depender de modelos de acceso tradicionales para defender sus infraestructuras.

Ante estos desafíos, numerosos proveedores de VPN tradicionales han comenzado a comercializar máquinas virtuales entregadas en la nube como soluciones de zero trust. Sin embargo, los servicios 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. Un ejemplo concreto: la industria fue testigo recientemente de picos masivos

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

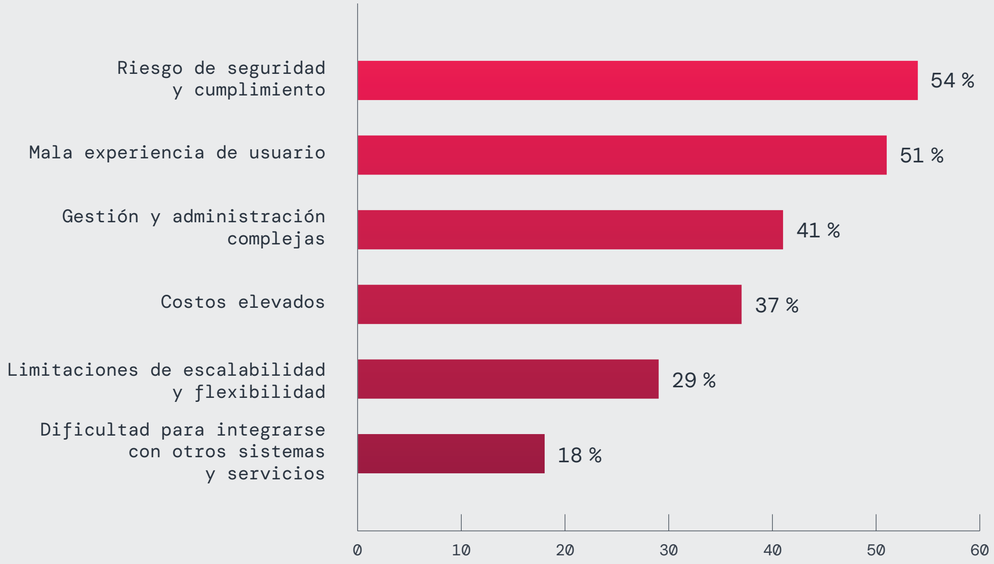


Figura 1: Los mayores desafíos con las soluciones VPN.

en la actividad de análisis 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 eres accesible, eres vulnerable a ataques, por eso, desde una perspectiva arquitectónica, la tecnología VPN basada en la nube nunca puede lograr verdaderos principios de zero trust, sin importar la marca.

Ransomware y VPN: una tormenta perfecta de riesgos

Los grupos de ransomware continúan explotando vulnerabilidades en las VPN con una precisión devastadora, aprovechando tanto fallos de día cero como debilidades conocidas antes de que las organizaciones puedan implementar 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 altos niveles de preocupación acerca del ransomware que ataca vulnerabilidades de VPN sin revisiones, lo que destaca la necesidad crítica de mecanismos de protección más potentes. Estos datos subrayan por qué las VPN ahora se consideran un lastre en lugar de herramientas confiables para mitigar los riesgos cibernéticos modernos.

Los ejemplos del mundo real continúan validando estos temores. En enero de 2023, varias organizaciones de asistencia sanitaria de EE. UU. fueron víctimas de un ataque de ransomware impulsado por una vulnerabilidad de Citrix NetScaler sin revisar (CVE-2023-4966). Este exploit permitió a los atacantes infiltrarse en los sistemas, interrumpir las operaciones del hospital, bloquear los registros de los pacientes y obligar a las instalaciones a desviar atención de emergencia crítica, todo porque la vulnerabilidad no había sido revisada a tiempo. Este incidente pone de relieve el riesgo generalizado que suponen las VPN sin revisiones. Los ciberdelincuentes analizan regularmente los sistemas expuestos, lo que garantiza que puedan aprovechar las vulnerabilidades antes de que las organizaciones apliquen correcciones, dejando a las organizaciones en riesgo de sufrir compromisos, interrupciones operativas y pérdidas financieras.

Las organizaciones deben abandonar la interminable rutina de revisiones y adoptar estrategias de defensa proactivas adaptadas a las amenazas en evolución. Los marcos de zero trust priorizan el control de acceso basado en la identidad y la verificación continua, lo que garantiza una reducción importante del riesgo de ransomware, incluso cuando las vulnerabilidades permanecen sin revisar. Los sistemas de detección automatizados y las políticas dinámicas contienen además posibles infracciones, impidiendo que los atacantes se muevan lateralmente o aumenten los privilegios.

¿Cuánto le preocupa sufrir un ataque de ransomware debido a vulnerabilidades sin revisiones?

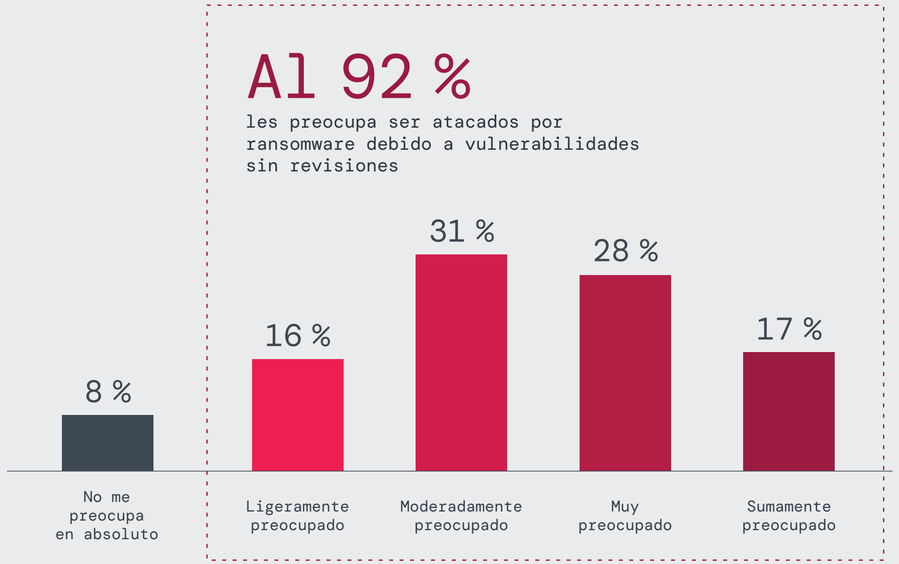


Figura 2: Preocupaciones sobre ataques de ransomware.

VPN y movimiento lateral: aumento del radio de explosión de las brechas

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 aumentar los privilegios e infiltrarse más profundamente en las redes objetivo, a menudo con consecuencias devastadoras.

Un total de 71 % de los encuestados expresó algún nivel de preocupación por este riesgo y un 32 % expresó altos niveles de preocupación. Estos sentimientos están justificados ya que las VPN generalmente otorgan un amplio acceso a la red, lo que permite a los atacantes moverse sin ser detectados, aumentar los privilegios y extraer 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, según confirmaron la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y el FBI. Los atacantes eludieron los controles administrativos, ejecutaron comandos arbitrarios, obtuvieron credenciales e implantaron shells web, lo que permitió el movimiento lateral a través de las redes. A pesar de incidentes de seguridad anteriores que involucraron a las VPN de Ivanti, estas nuevas vulnerabilidades demuestran que revisar o rediseñar las soluciones VPN tradicionales sigue sin lograr resolver los fallos de seguridad fundamentales inherentes a los modelos de acceso remoto basados en red.

¿Hasta qué punto está preocupado de que los atacantes se muevan lateralmente a través de su red si una VPN se ve comprometida?

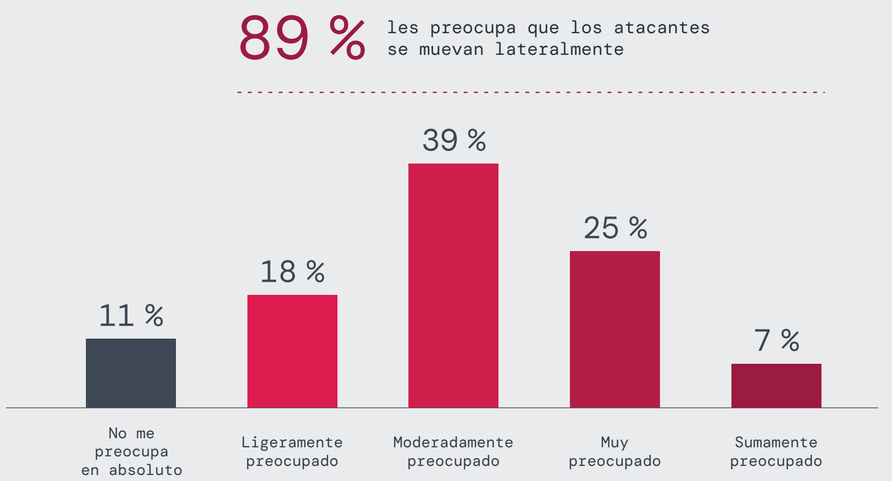


Figura 3: Preocupaciones empresariales que se moverán lateralmente a través de la red si una VPN se ve comprometida.

Para mitigar estos riesgos, las organizaciones deben pasar del acceso basado en VPN al acceso a red de zero trust (ZTNA) con una segmentación estricta. A diferencia de las VPN, que otorgan a los usuarios un amplio acceso a la red, ZTNA proporciona acceso a nivel de aplicación basado en la identidad y el contexto, lo que garantiza que los usuarios únicamente puedan acceder a los recursos específicos que necesitan. Este enfoque impide el movimiento lateral incluso si los atacantes obtienen acceso inicial, lo que reduce drásticamente la superficie de ataque y el radio de explosión potencial de las infracciones. Además, la implementación de redes y microsegmentación fortalece la seguridad al aislar sistemas críticos y prevenir la comunicación no autorizada entre activos comprometidos y seguros.

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 debería 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 dañinas, ya que los ciberdelincuentes pueden explorar fácilmente la infraestructura VPN afectada y explotarla antes de que se publique o aplique cualquier revisión. La notificación de CVE es beneficiosa, ya que este esfuerzo comunitario ayuda a proveedores y clientes a seguir las mejores prácticas y a mejorar su ciberseguridad mediante la aplicación de revisiones y la divulgación. La forma en que se descubren estas CVE y la información que contienen refleja los cambios en el cambiante panorama de amenazas.

Zscaler ThreatLabz analizó 411 vulnerabilidades y exposiciones comunes (CVE) de VPN entre 2020 y 2025, según lo informado por el Programa CVE de MITRE. Los resultados indican un incremento de vulnerabilidades de VPN que han aumentado gradualmente durante la primera mitad de esta década. Estas CVE cubren una amplia gama de fallos 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 fallos criptográficos y ataques DoS y DDoS. No faltan vulnerabilidades recientes de VPN, muchas de las cuales han provocado infracciones de seguridad importantes y muy visibles.

Muchos de estos CVE son críticos. En 2024, por ejemplo, el 60 % de las 83 vulnerabilidades de VPN reportadas 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, muchas de estas CVE eran exploits de día cero. Si bien las CVE en 2025 aún son bajas a principios de año, ya se han revelado vulnerabilidades importantes, como dos exploits de día cero: CVE-2025-0282 y CVE-2025-0283.

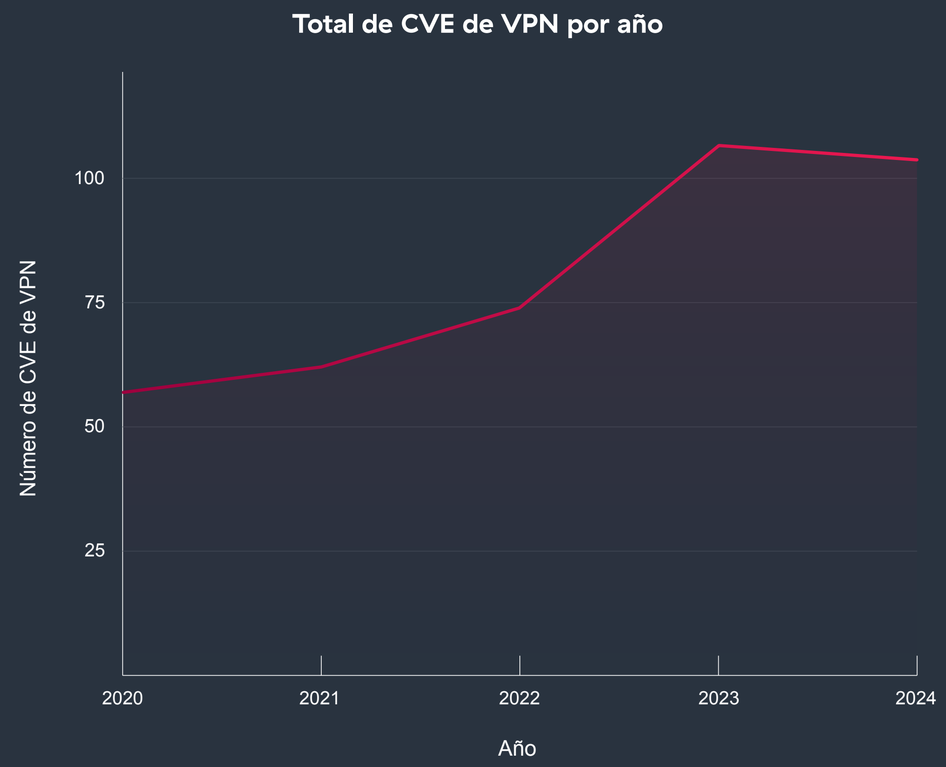


Figura 4: Total de CVE de VPN para cada año, de 2020 a 2024.

1. RCE sigue siendo la principal amenaza

- **Observación:** las vulnerabilidades RCE encabezan la lista durante los cuatro años, con 32 solo en 2024. RCE representa 149 CVE, incluidos los datos de 2025, lo que lo convierte en el tipo de vulnerabilidad más frecuente y crítico.
- **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 revisiones y la protección de los sistemas vulnerables.

2. La escalada de privilegios crece constantemente con el tiempo

- **Observación:** hay un aumento constante en las 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 de denegación de servicio (DoS) muestran un marcado aumento del 200 %

- **Observación:** las 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 filtración 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 supervisión del tráfico para detectar y prevenir filtraciones de datos.

5. Crecimiento constante de las vulnerabilidades de omisión de autenticación

- **Observación:** los incidentes de evasión de autenticación han sido relativamente bajos, pero consistentes, y aumentaron de 4 en 2020 a un pico de 6 en 2023 y a 4 vulnerabilidades en 2024, totalizando 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 omisiones de autenticación. Hay que tener en cuenta que algunas categorías son agrupaciones generales para tipos de ataques separados, pero estrechamente relacionados: por ejemplo, la omisión de autenticación incluye ataques que pueden omitir la autenticación de segundo factor o multifactor (MFA), mientras que otros omiten las medidas de autenticación básicas. En general, cualquier vulnerabilidad de RCE será un elemento de alta prioridad a remediar para cualquier organización.

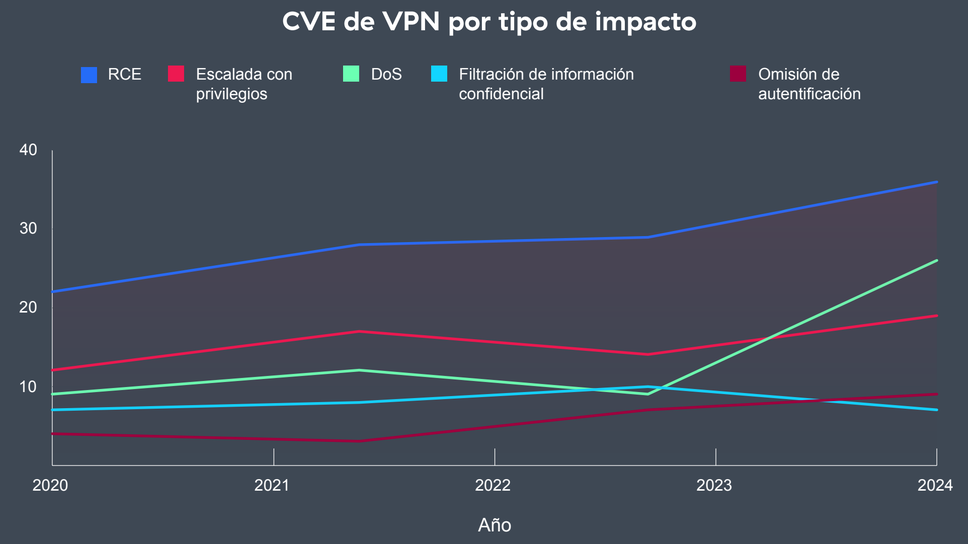


Figura 5: el tipo de impacto de las CVE de VPN de 2020 a 2024, que abarca RCE, escalada de privilegios, filtración de información confidencial de DoS y omisión de autenticación.

Tendencias clave: vulnerabilidades críticas de VPN

Además 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 ALTAS o CRÍTICAS aumentaron un 38,9 % entre 2020 y 2024.** De hecho, el 66,3 % de todos las CVE en 2024 se clasificaron como ALTAS o CRÍTICAS, lo que indica un posible impacto grave para las organizaciones cuando se explotan antes de que se apliquen las revisiones. Además, ThreatLabz analizó las tendencias críticas en diferentes tipos de vulnerabilidades representadas en los datos de CVE que las empresas deberían comprender para protegerse mejor contra las amenazas emergentes de VPN.

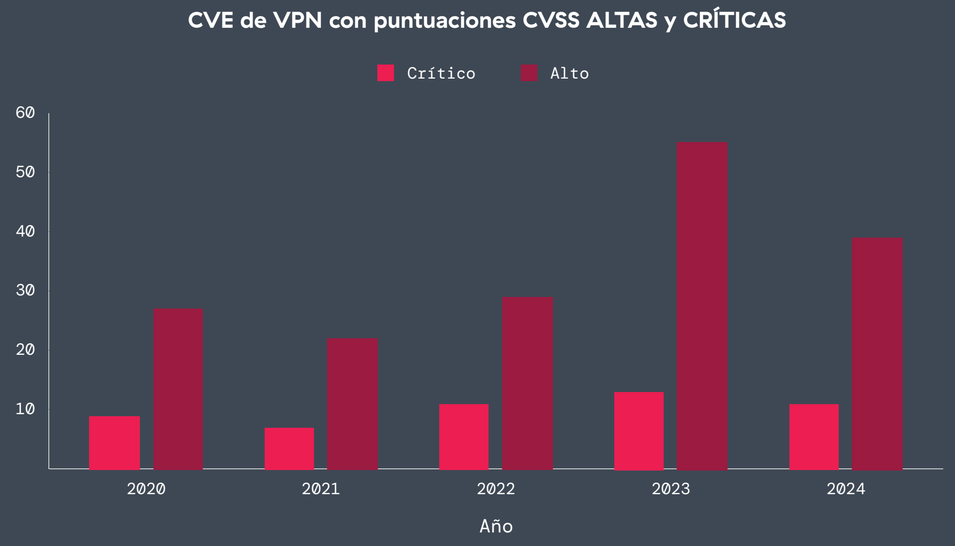


Figura 6: El volumen de CVE de VPN con puntuaciones CVSS ALTAS y CRÍTICAS de 2020 a 2024.

1. Aumento de la explotación de las interfaces

- **Tendencia:** las vulnerabilidades de inyección de comandos y validación de entrada han ido aumentando 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. Dado que estas interfaces están inherentemente expuestas a Internet a través de su arquitectura, son propensas a ser explotadas por ciberdelincuentes.
- **Escalada:** si bien estas vulnerabilidades ya estaban presentes en 2020–2021, se intensificaron significativamente a partir de 2022, lo que sugiere que los atacantes ven estas interfaces de administración como objetivos atractivos y accesibles, especialmente debido a prácticas de codificación de seguridad inadecuadas.

2. Autenticación generalizada y omisiones de MFA

- **Tendencia:** los ataques dirigidos específicamente a métodos de autenticación (incluidas las omisiones de MFA, el secuestro de sesiones y la gestión inadecuada de sesiones) aumentaron de manera constante.
- **Escalada:** en los años anteriores (2020–2021) se observaron principalmente omisiones de autenticación más simples, mientras que entre 2023 y 2025, estas evolucionaron hacia ataques más avanzados, automatizados y persistentes dirigidos explícitamente a las debilidades de MFA, lo que indica la intención de los atacantes de socavar medidas de seguridad más sólidas.

3. Aumento de los exploits de escalada de privilegios locales

- **Tendencia:** las vulnerabilidades de escalada de privilegios locales 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 y se convirtió en métodos de escalada de privilegios más sofisticados, como el secuestro de DLL, que otorga a los atacantes un acceso más profundo a nivel del sistema.

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. Fallos criptográficos persistentes e intensificados

- **Tendencia:** los problemas relacionados con la implementación criptográfica (como validación incorrecta de certificados, claves filtradas 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 fallos 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.

Preocupaciones sobre la seguridad de las VPN (cont.)

Los desafíos de implementar 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 pone de relieve estos desafíos: el 51 % de las organizaciones anticipan o enfrentan complejidad de configuración. Además, el 39 % informa una falta de experiencia y recursos, mientras que el 24 % enfrenta cuellos de botella en el rendimiento, lo que indica que las arquitecturas de red heredadas están mal equipadas para soportar los controles de acceso granulares requeridos para los entornos de TI actuales.

Los desafíos de segmentación desempeñaron un papel notable en el ataque de ransomware a MGM Resorts en 2023, donde los atacantes obtuvieron acceso inicial a través de ingeniería social, pero pudieron moverse lateralmente debido a una segmentación insuficiente. La infracción interrumpió las operaciones del hotel, los cajeros automáticos y los sistemas de juego del casino, lo que costó a la empresa unos 100 millones de dólares estadounidenses en daños. Este caso resalta cómo una segmentación deficiente permite a los atacantes pasar de un sistema crítico a otro, amplificando el impacto de una intrusión inicial.

Para abordar estos desafíos, las organizaciones deben implementar modelos de segmentación basados en la nube e impulsados por la identidad que agilicen la aplicación de políticas y reduzcan la sobrecarga manual. A diferencia de la segmentación de red tradicional, que se basa en reglas de cortafuegos complejas y configuraciones de VLAN, un enfoque de zero trust permite una segmentación dinámica basada en la identidad del usuario, la postura del dispositivo y evaluaciones de riesgos en tiempo real. Esto garantiza que sólo los usuarios autorizados puedan acceder a aplicaciones específicas y al mismo tiempo mantiene segura la red más amplia.

¿Qué problemas encontró o previó su organización mientras se implementaba la segmentación?

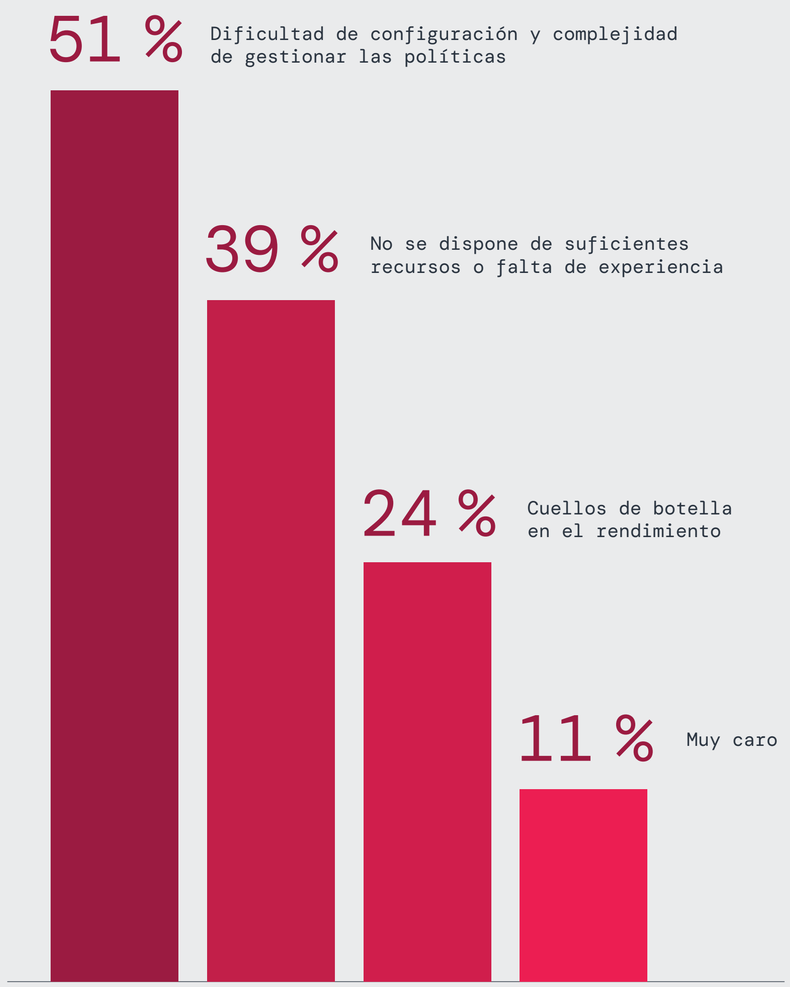


Figura 7: los principales desafíosa los que se enfrentan las empresas al implementar la segmentación.

Las VPN aumentan los riesgos de ciberseguridad en fusiones y adquisiciones

Más allá de los desafíos de seguridad cotidianos, las transiciones de TI importantes, como las fusiones y adquisiciones, plantean riesgos adicionales y amplían las superficies de ataque. Estas transiciones a menudo implican la fusión de redes, aplicaciones e identidades dispares, lo que puede generar 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 filtración de datos de Capita de 2023, en la que los atacantes explotaron las debilidades de seguridad posteriores a una adquisición corporativa y obtuvieron acceso no autorizado a datos confidenciales. El incidente se debió a políticas de seguridad desalineadas entre las entidades fusionadas, lo que permitió a los ciberdelincuentes moverse lateralmente a través de la red recién integrada. Esta brecha subraya cómo los controles de seguridad inconsistentes, el acceso a VPN heredadas y los entornos no segmentados crean condiciones ideales para los ciberataques durante una actividad de fusiones y adquisiciones.

Para mitigar estos riesgos durante fusiones y adquisiciones, las organizaciones deben priorizar la debida diligencia en materia de ciberseguridad, aplicar el acceso con privilegios mínimos e implementar la segmentación. A diferencia de los modelos de acceso basados en VPN, la zero trust evita que los entornos de TI fusionados hereden permisos de acceso amplios, lo que reduce efectivamente el riesgo de movimiento lateral y escalada de privilegios. Al reemplazar las VPN y las defensas basadas en el perímetro con controles de acceso basados en la identidad que validan cada solicitud, las organizaciones pueden proteger los entornos de TI heredados y recientemente integrados.

¿Le preocupa ser vulnerable a ataques de ciberseguridad después de fusiones y adquisiciones?

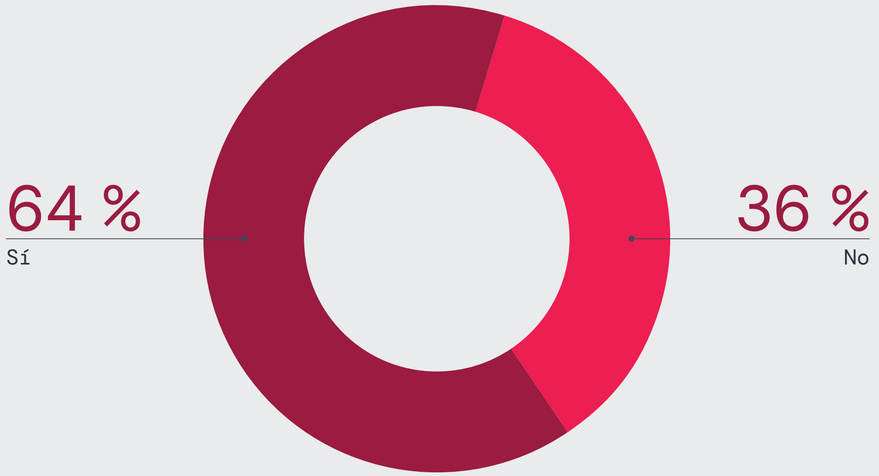


Figura 8: las empresas están preocupadas por los ciberataques después de fusiones y adquisiciones

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, dependen de un amplio acceso a la red una vez que se completa 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 aprovechar credenciales robadas o débiles, configuraciones incorrectas y vulnerabilidades sin revisiones para secuestrar estas conexiones confiables. Con un 93 % de encuestados expresando inquietudes críticas acerca de las vulnerabilidades de puerta trasera, el acceso de terceros representa una bomba de relojería para las organizaciones que dependen de modelos de acceso estáticos y basados en la confianza.

Y tienen motivos para estar preocupados. En agosto de 2024, Enterprise Financial Group (EFG) sufrió una importante infracción de datos que expuso la información personal de casi 20 000 clientes. La infracción se remonta a vulnerabilidades en 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 las VPN de terceros e implementar controles de políticas más estrictos, como el acceso con límite de tiempo, la inspección de tráfico de extremo a extremo (de dispositivo a aplicación) y la autenticación adaptativa. La transición a un modelo de zero trust permitirá la aplicación del acceso específico a cada aplicación, garantizando que los socios externos únicamente tengan el acceso mínimo necesario. Además, la supervisión continua y las políticas basadas en riesgos pueden mitigar significativamente las vulnerabilidades de terceros.

¿Hasta qué punto está preocupado por los terceros que actúan como posibles puertas traseras para que los atacantes entren en su red a través de su acceso VPN?

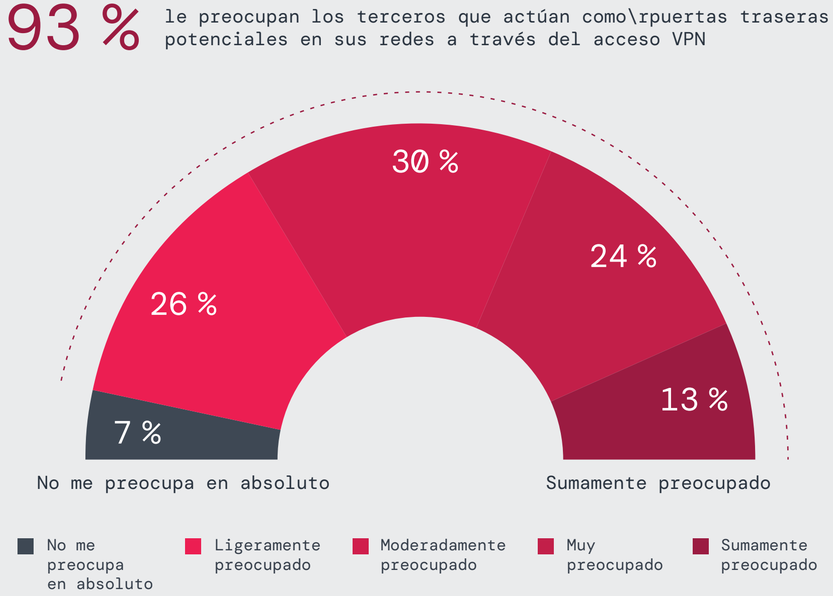


Figura 9: Las empresas se preocupan por el acceso a VPN de terceros que facilita los ataques cibernéticos.

Desafíos y brechas con medidas de protección heredadas

Las herramientas tradicionales quedan expuestas para aplicaciones privadas

Proteger las aplicaciones privadas frente a amenazas web cada vez más sofisticadas, como ransomware, robo de credenciales y abuso de API, se ha convertido en una prioridad fundamental para las empresas modernas. Sin embargo, muchas organizaciones siguen confiando en herramientas heredadas deficientes para afrontar el panorama de amenazas actual.

Según la encuesta, los cortafuegos (84 %), cortafuegos de aplicaciones web (WAF, 58 %) y VPN (43 %) siguen dominando las defensas de las organizaciones frente a ataques web. Sin embargo, los atacantes eluden cada vez más estas herramientas (aprovechando dispositivos sin parches, configuraciones deficientes y debilidades inherentes en los modelos de seguridad basados en el perímetro), lo que demuestra que estas defensas tradicionales ya no satisfacen las demandas de los paisajes de amenazas modernos.

Las brechas recientes ponen de relieve las deficiencias de estas defensas perimetrales. En agosto de 2024, hackers chinos, un grupo conocido como Salt Typhoon, se infiltraron en importantes empresas de telecomunicaciones estadounidenses, incluidas AT&T y Verizon, explotando vulnerabilidades en dispositivos de red y enrutadores sin revisiones. Este ataque comprometió metadatos confidenciales de más de un millón de usuarios, lo que demuestra cómo los atacantes sofisticados pueden eludir las medidas de seguridad tradicionales, como los cortafuegos y las VPN.

La única solución viable para proteger eficazmente las aplicaciones privadas es superar las anticuadas defensas perimetrales y adoptar modelos de acceso de zero trust. Las arquitecturas de zero trust eliminan la dependencia de la seguridad basada en la red, permitiendo a los usuarios conectarse directamente a las aplicaciones bajo políticas rigurosas de acceso granular y con privilegios mínimos. A diferencia de los cortafuegos y las VPN, las arquitecturas de zero trust permiten a los usuarios conectarse directamente a las aplicaciones con acceso granular y con privilegios mínimos. Este enfoque bloquea los intentos de acceso no autorizado y previene el movimiento lateral, el secuestro de sesiones y el robo de credenciales, tácticas que los atacantes suelen utilizar para eludir las defensas perimetrales tradicionales.

¿Qué productos utiliza para proteger sus aplicaciones privadas frente a ataques basados en la web?

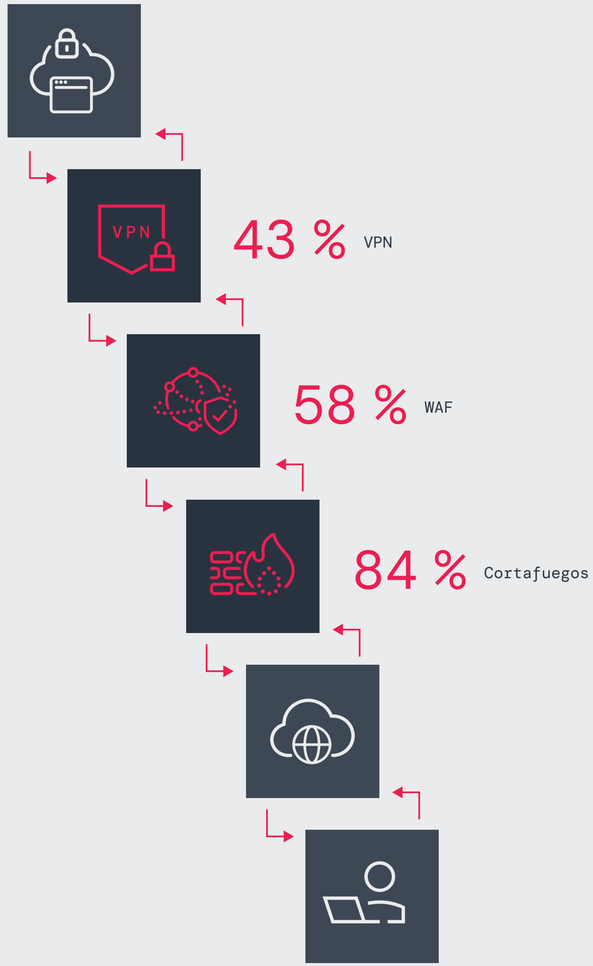


Figura 10: Los productos de seguridad que utilizan las empresas para defender sus aplicaciones privadas de las amenazas basadas en la web.

Implementación de NAC en entornos VPN: una protección limitada

Un notable 54 % de las organizaciones encuestadas informan que utilizan NAC para proteger el acceso VPN a recursos privados. Sin embargo, estas implementaciones aún no han podido evitar las infracciones y vulnerabilidades comúnmente asociadas con las vulnerabilidades de VPN, lo que resalta la incapacidad de NAC para abordar los riesgos sistémicos de los modelos de confianza basados en la red.

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

Las infracciones recientes demuestran que, incluso con NAC implementado, las vulnerabilidades de VPN siguen siendo una debilidad crítica. En noviembre de 2023, el Departamento de Energía de EE. UU. confirmó un importante incidente de seguridad que involucraba credenciales VPN comprometidas, que permitía a los atacantes eludir los controles de acceso e infiltrarse en sistemas internos confidenciales. Esto pone de manifiesto cómo los atacantes pueden explotar las debilidades de la VPN directamente, ya sea a través de credenciales robadas, vulnerabilidades sin revisar o secuestro de sesiones, lo que hace que NAC sea una defensa incompleta si el modelo de confianza subyacente permanece sin cambios.

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

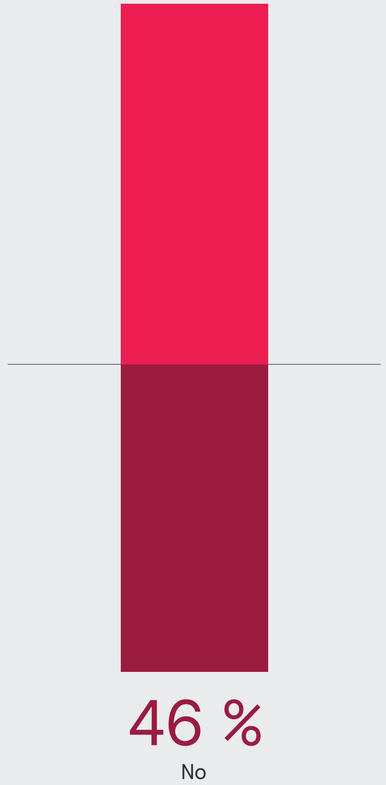


Figura 11: Proporción de empresas que utilizan NAC entre VPN y recursos privados.

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

Experiencia de usuario de VPN_ y problemas de_gestión

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

Las VPN no sólo son una responsabilidad en términos de seguridad: también son una fuente importante de insatisfacción de los usuarios. Los usuarios finales expresan cada vez más frustraciones con los problemas de rendimiento de la VPN, que crean obstáculos para la productividad y aumentan la creciente presión sobre los equipos de TI.

Las velocidades de conexión lentas son la queja más común (23 %), lo que subraya la reputación de las VPN de latencia, congestión y bajo rendimiento al acceder a aplicaciones en la nube desde casa. Los problemas de autenticación también siguen siendo un problema importante: el 20 % de los encuestados cita procesos de inicio de sesión complejos y el 17 % tiene dificultades para acceder a las aplicaciones debido a errores de autenticación.

Estos problemas de rendimiento alteran las operaciones comerciales diarias, reducen la productividad y convierten el servicio de asistencia técnica de TI en un cuello de botella a medida que los equipos luchan con frecuentes solicitudes de resolución de problemas, una situación que sólo empeora a medida que los entornos de trabajo remotos e híbridos aumentan en complejidad.

Reemplazar las VPN con acceso a red de zero trust (ZTNA) no sólo elimina la congestión del ancho de banda, sino que también mejora enormemente la experiencia del usuario final al permitir conexiones directas, seguras y sin latencia a las aplicaciones. A diferencia de las VPN, que enrutan todo el tráfico a través de una puerta de enlace central y crean cuellos de botella en el rendimiento, ZTNA permite el acceso directo y seguro a las aplicaciones sin degradación del rendimiento. Al adoptar controles de acceso basados en la identidad, verificación continua y seguridad entregada en la nube, las organizaciones no sólo pueden eliminar las frustraciones comunes de VPN, sino también aumentar la productividad del personal y reducir la carga de TI de solucionar problemas y brindar soporte a marcos de VPN inflexibles.

¿Cuál es la queja más común de sus usuarios al acceder a aplicaciones a través de VPN?

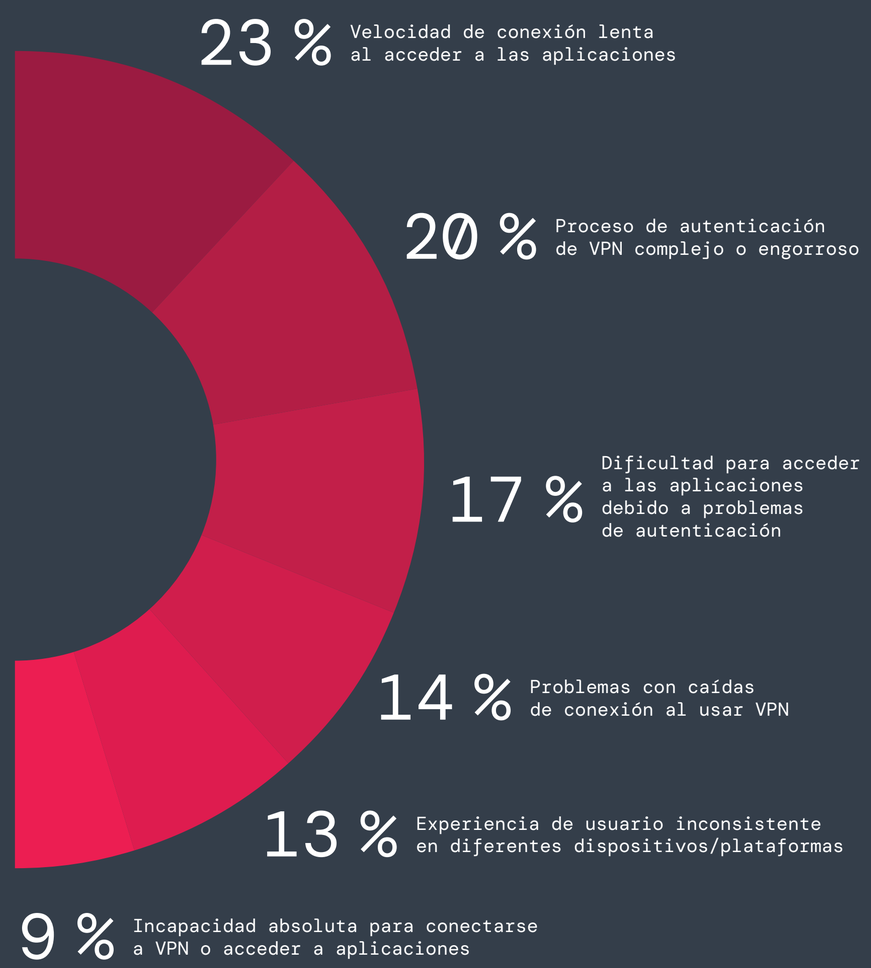


Figura 12: Las quejas más comunes entre los usuarios de VPN.

Gestión de VPN: sobrecargando a los equipos de TI y exponiendo vulnerabilidades

Las VPN están sobrecargando a los equipos de TI con vulnerabilidades de seguridad persistentes, demandas de mantenimiento que requieren muchos recursos y modelos de acceso obsoletos que ya no se alinean con las necesidades de los entornos empresariales actuales centrados en la nube. La principal preocupación entre estos equipos (52 %) son las brechas de seguridad que darán lugar a incidentes de seguridad, lo que subraya los riesgos actuales relacionados con el robo de credenciales, las vulnerabilidades de software sin revisiones y los atacantes que aprovechan el acceso VPN para realizar movimientos laterales sin control. Estos riesgos ponen de relieve por qué las VPN están consideradas cada vez más como soluciones de acceso con gran riesgo de sufrir daños.

Las VPN se han convertido en una carga financiera y operativa para los equipos de TI, y el 41 % de los encuestados destaca los exorbitantes costes de recursos vinculados a su mantenimiento. El ciclo incesante de aplicación de revisiones, resolución de problemas y supervisión de registros es necesario para proteger una infraestructura obsoleta, pero deja a los equipos sobrecargados e incapaces de concentrarse 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 otorgar acceso preciso y basado en la identidad a aplicaciones específicas, las VPN a menudo brindan conectividad de red amplia y sin restricciones, lo que aumenta drásticamente el potencial de amenazas internas y movimiento lateral por parte de los atacantes. Además, el 26 % menciona los costes operativos de administrar concentradores VPN y otros dispositivos, lo que ilustra la complejidad de mantener dispositivos de hardware, túneles de red y puertas de enlace de acceso para sostener 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.

¿Cuáles son las inquietudes más comunes de su equipo de TI/ seguridad al utilizar VPN?

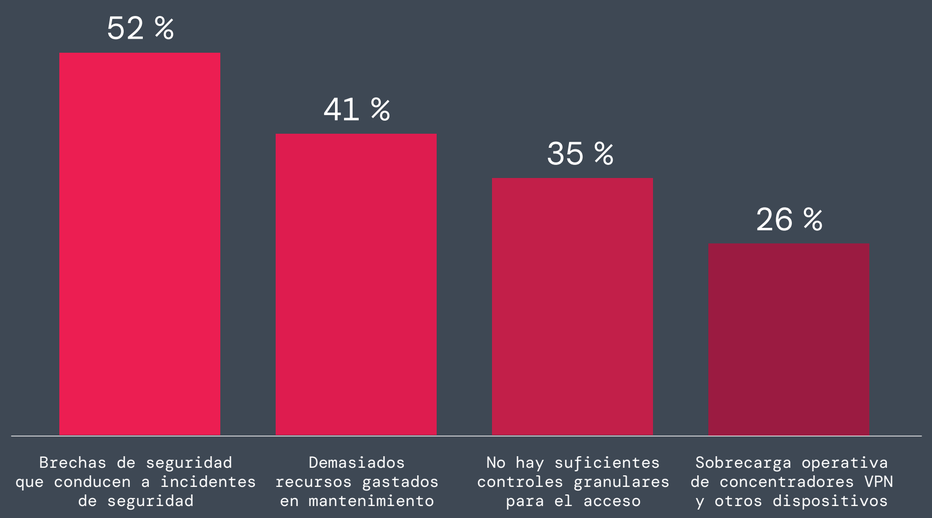


Figura 13: Las principales preocupaciones de los equipos de TI y seguridad al dar soporte a las VPN.

Para abordar estos desafíos, las organizaciones deben pasar del acceso VPN basado en red a un modelo de zero trust distribuido 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 liberan de la carga de las tareas de mantenimiento constante, lo que les permite centrarse en iniciativas de seguridad proactivas y, al mismo tiempo, brindar experiencias de usuario más rápidas y fluidas.

La pesada carga de la gestión de VPN

La gestión de la infraestructura de VPN continúa ejerciendo presión sobre los equipos de TI, y las principales preocupaciones se centran en la confiabilidad, el rendimiento y los gastos generales de mantenimiento. La solución de problemas de conectividad y estabilidad de la VPN sigue siendo el principal desafío, citado por el 54 % de los encuestados. Los equipos de TI tienen dificultades para mantener un tiempo de actividad constante de la VPN, y los fallos de conexión generan interrupciones generalizadas que degradan la productividad, comprometen la seguridad y frustran a los empleados.

Equilibrar el rendimiento de la VPN y la experiencia del usuario sigue siendo un desafío importante (50 %) dado que las VPN a menudo introducen latencia, desconexiones y velocidades inconsistentes, especialmente en entornos que priorizan la nube. Además, el 47 % de los profesionales de TI destacan las frecuentes demandas de parches y los costes de recursos como un obstáculo importante, lo que pone de relieve los desafíos operativos de mitigar vulnerabilidades persistentes y mantener sistemas obsoletos.

Estos desafíos han jugado un papel en varias infracciones 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 reparación de una vulnerabilidad ampliamente conocida permitieron a los ciberdelincuentes explotar un software VPN obsoleto y obtener acceso no autorizado a la red. Este caso resalta la insuficiencia de los ciclos de aplicación de revisiones reactivas, incluso entre organizaciones con equipos de TI dedicados, y demuestra cómo las defensas VPN incompletas exponen 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 revisiones de seguridad y la optimización del rendimiento, las organizaciones deben reevaluar la viabilidad a largo plazo del acceso basado en VPN. Al reemplazar los concentradores VPN y los dispositivos de red como cortafuegos y NAC con una arquitectura nativa de la nube, los equipos de TI pueden eliminar los cuellos de botella de la infraestructura, reducir los ciclos de revisiones y eliminar la necesidad de solucionar manualmente los problemas de conexión.

El acceso con privilegios mínimos basado en políticas garantiza que los usuarios se conecten exclusivamente a aplicaciones autorizadas, sin la carga de administrar reglas de cortafuegos complejas o políticas de segmentación de red. Al realizar la transición a un modelo de zero trust distribuido en la nube, las empresas podrán eliminar los cuellos de botella relacionados con las VPN y, al mismo tiempo, garantizar un acceso fluido y basado en políticas a las aplicaciones, sin la carga de gestionar la infraestructura de red, revisiones de software o esfuerzos de escalamiento complejos.

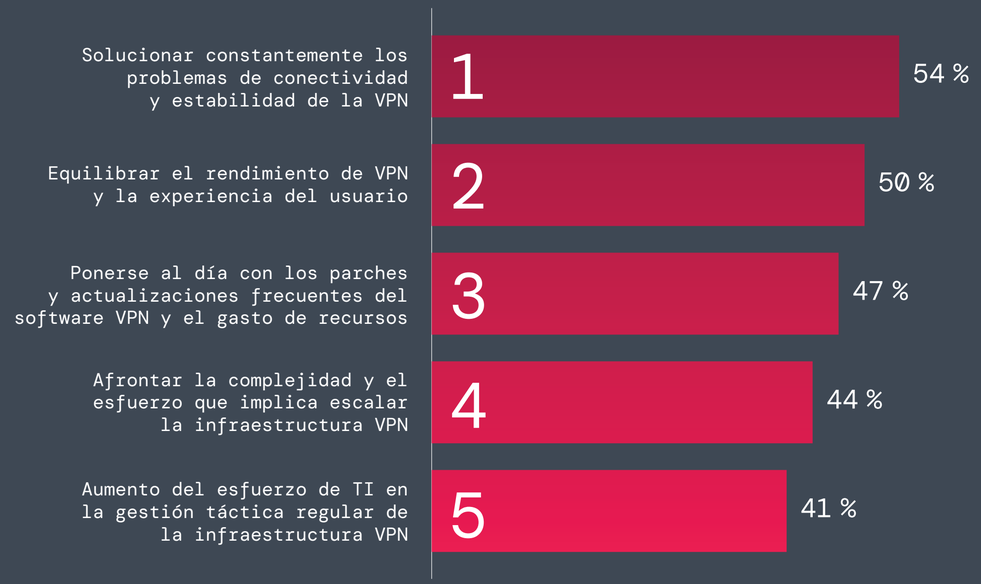


Figura 14: Las principales preocupaciones entre los equipos de TI que gestionan la infraestructura VPN.

Controles de acceso 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 acceso preciso y específico para cada aplicación, muchas organizaciones aún otorgan acceso amplio a la red y confían en modelos de confianza implícitos, dejando expuestos los sistemas críticos.

Los resultados de la encuesta revelan que el 52 % de las organizaciones aún dependen de modelos de acceso obsoletos, como reglas de cortafuegos de red estáticas (28 %) o acceso abierto para usuarios autenticados (24 %). Estos controles obsoletos hacen que sea fácil para los atacantes viajar por las redes sin ser detectados, escalar privilegios y exfiltrar datos críticos una vez que obtienen acceso.

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

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

¿Cómo define el acceso de los usuarios de VPN a las aplicaciones?

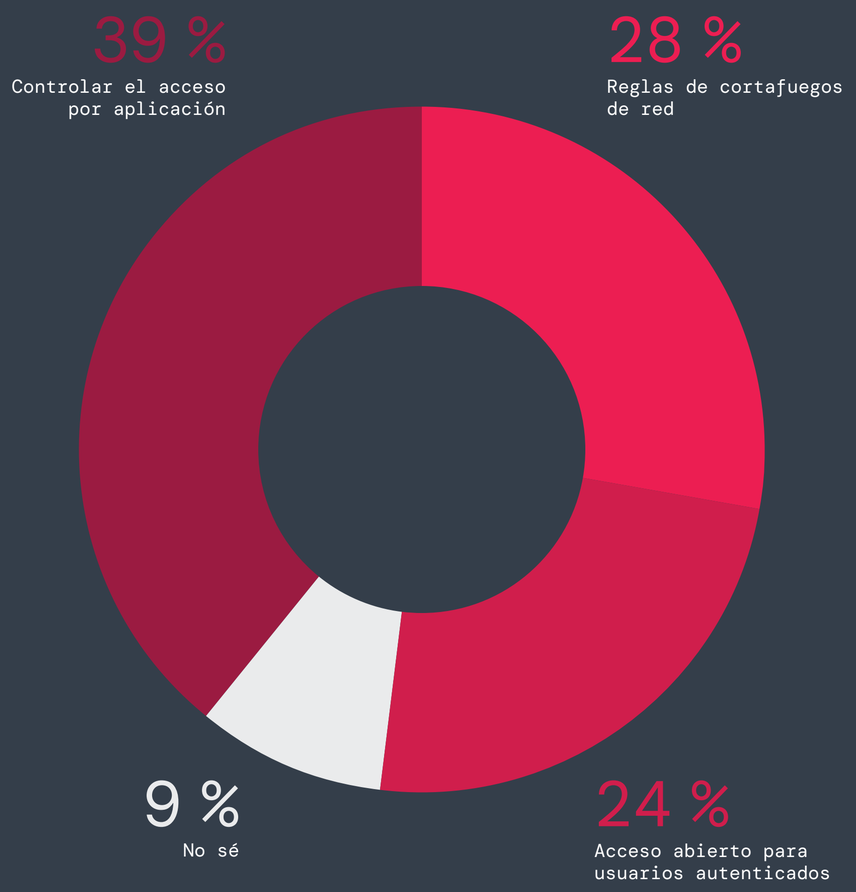


Figura 15: Las formas en que las empresas definen el acceso de los usuarios de VPN a las aplicaciones.

Reemplazo de VPN: un cambio hacia el acceso seguro

Las crecientes vulnerabilidades de seguridad, las dificultades en la experiencia del usuario y los altos costes de mantenimiento de las VPN están impulsando a las organizaciones a acelerar su transición a tecnologías de acceso seguro modernas como ZTNA. Este cambio señala el convencimiento cada vez más extendido de que las VPN ya no son capaces de satisfacer las demandas operativas o de seguridad modernas.

La encuesta confirma este impulso: el 65 % de los encuestados afirma que sus organizaciones están reemplazando o tienen previsto reemplazar sus VPN durante el próximo año.

A medida que las organizaciones se alejan cada vez más de las VPN, deben priorizar la adopción de modelos de seguridad entregados desde la nube que refuercen el acceso granular a nivel de aplicación en lugar de una amplia conectividad de red. ZTNA elimina los riesgos relacionados con VPN al garantizar que los usuarios únicamente puedan acceder a los recursos que necesitan, en función de su identidad y postura de seguridad, sin tener que colocarlos nunca en la red corporativa. Este enfoque mejora la seguridad, reduce la complejidad operativa y mejora la experiencia del usuario, lo que hace que el reemplazo de VPN sea un paso urgente y necesario para las empresas modernas.

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

65 %

de las organizaciones tienen un plan para reemplazar sus servicios VPN existentes

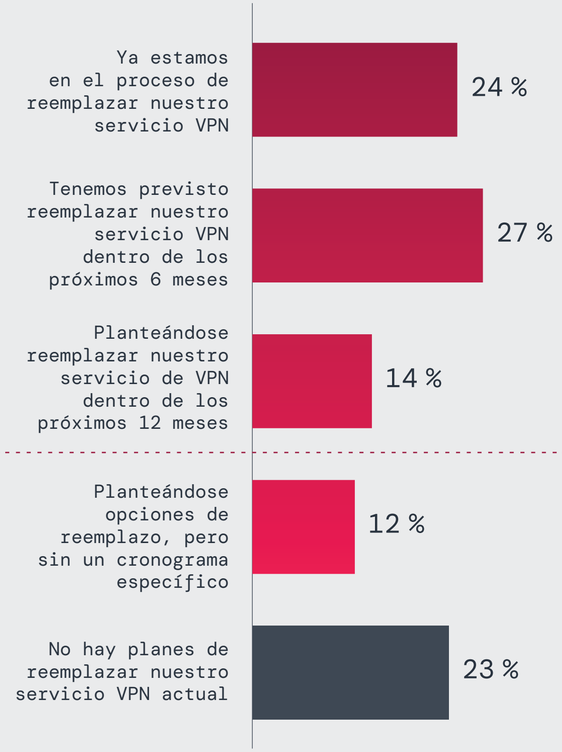
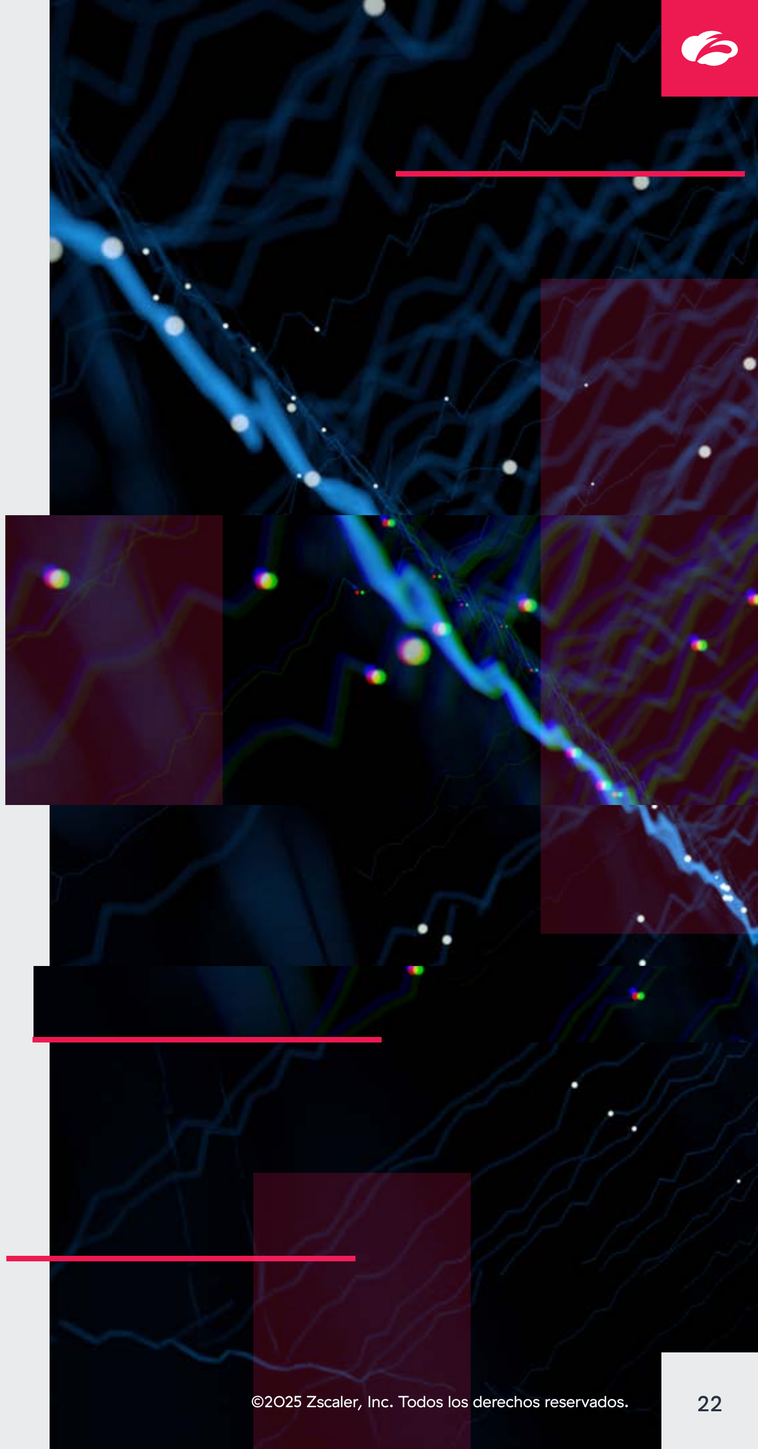


Figura 16: Planes empresariales para reemplazar los servicios VPN existentes.



Adopción de zero trust

Zero Trust reemplaza a las VPN a gran escala

A medida que se acelera la tendencia de reemplazo de VPN, la gran mayoría de las organizaciones están recurriendo a arquitecturas de zero trust para habilitar controles de acceso granulares, reducir sus superficies de ataque y mejorar la productividad de los usuarios. Los resultados de la encuesta subrayan el impulso creciente de este cambio de paradigma: el 81 % de los encuestados indica que tiene planes de adoptar la zero trust dentro del año. Entre ellos, el 35 % ya está implementando soluciones de zero trust, el 24 % tiene previstas implementaciones dentro de seis meses y el 22 % cuenta con estrategias de implementación planificadas para el año siguiente, lo que demuestra que zero trust es la estrategia líder del sector para reemplazar tecnologías de acceso heredadas como las VPN.

La adopción exitosa de zero trust requiere alineación entre los equipos de seguridad y las operaciones comerciales. Las organizaciones deben realizar evaluaciones de riesgos para identificar sus puntos de acceso más vulnerables (ya sea acceso remoto, integraciones de terceros o aplicaciones críticas) y priorizar la implementación de zero trust en consecuencia. Aprovechar la automatización para la aplicación de políticas puede acelerar la transición y, al mismo tiempo, reducir los gastos administrativos.

¿Cuáles son sus planes para adoptar una estrategia de confianza cero para su organización?

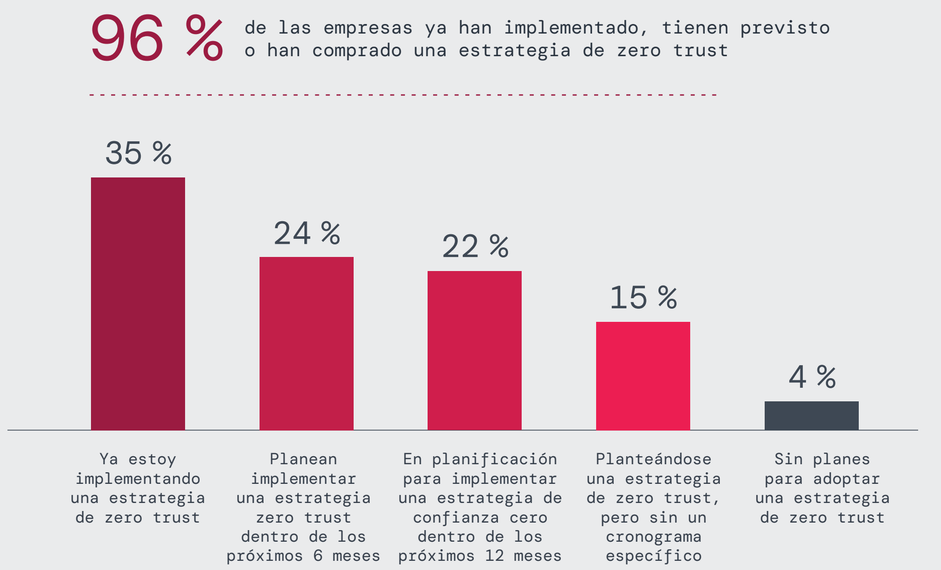


Figura 17: Planes empresariales para implementar una estrategia de zero trust.

Prioridades de Zero Trust: el trabajo remoto impulsa la adopción

El abandono de las VPN tradicionales subraya una transformación significativa: las organizaciones están recurriendo a arquitecturas de zero trust para abordar las brechas de seguridad, optimizar las operaciones de TI y satisfacer las demandas del personal remoto descentralizado. 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 proteger al personal remoto es la principal motivación para este cambio: el 37 % de las organizaciones se centran en el trabajo remoto y el 28 % en la seguridad del personal híbrido. Este movimiento refleja una tendencia más amplia hacia modelos de seguridad que ofrecen acceso directo a aplicaciones específicas, reduciendo así las complejidades asociadas con la gestión de múltiples productos puntuales inherentes a las configuraciones VPN heredadas.

La implementación de un marco de zero trust no sólo fortalece la seguridad, sino que también alivia la carga operativa de administrar numerosas soluciones de seguridad. Al unificar las políticas y controles de seguridad en un sistema cohesivo, las organizaciones pueden reducir los gastos administrativos y agilizar las operaciones. Por ejemplo, una plataforma zero trust que realiza múltiples acciones de políticas en un único análisis puede eliminar la necesidad de encadenar varias soluciones, lo que simplifica la experiencia del usuario y mantiene una seguridad sólida.

Para proteger eficazmente al personal remoto e híbrido con una arquitectura de zero trust, las organizaciones deben centrarse en integrar medidas de seguridad que minimicen la complejidad. La implementación de una plataforma de zero trust unificada puede consolidar varias funciones de seguridad, reduciendo la necesidad de múltiples productos puntuales y simplificando la gestión. Este enfoque mejora la seguridad y la eficiencia operativa, permitiendo que los equipos de TI se concentren en iniciativas estratégicas en lugar de administrar una compleja variedad de herramientas de seguridad.

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

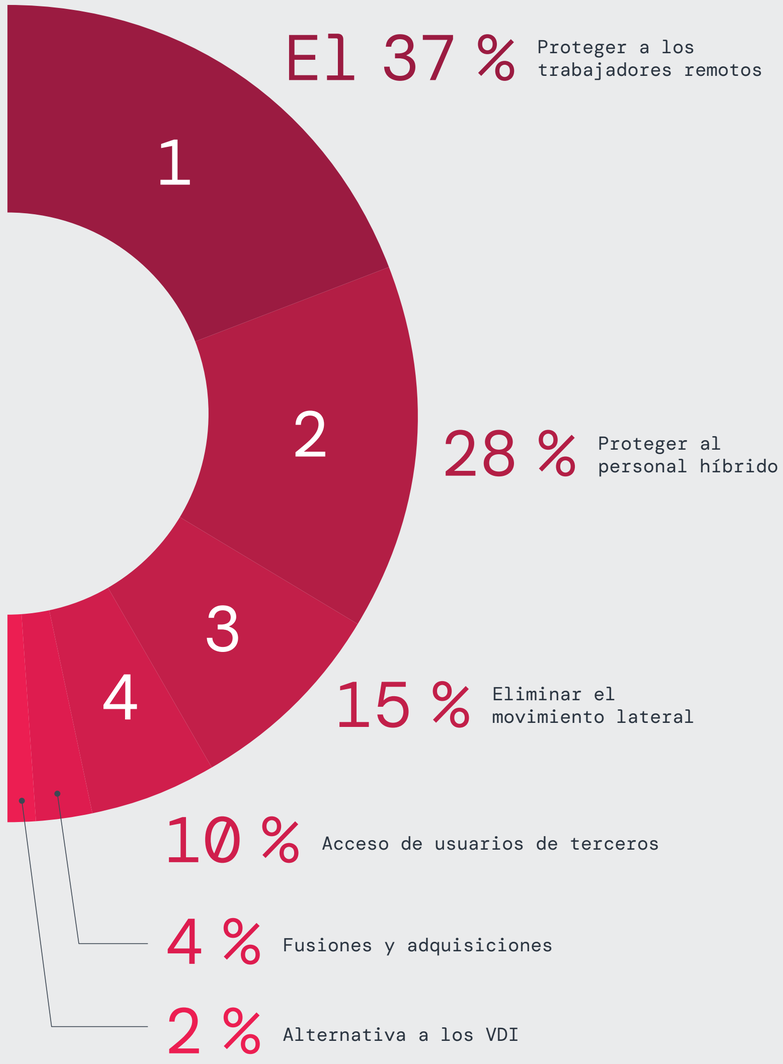


Figura 18: Casos de uso principales de las empresas para soluciones zero trust.

Ventajas clave de reemplazar las VPN con Zero Trust

La adopción de soluciones de zero trust está transformando la seguridad empresarial y brindando beneficios de gran alcance más allá del acceso seguro, en particular al simplificar la administración, mejorar el rendimiento y la escalabilidad, reducir drásticamente la superficie de ataque y mejorar la eficiencia de los recursos. Las organizaciones que reemplazan los modelos VPN con zero trust no sólo están actualizando sus herramientas; también están preparando toda su estrategia de acceso remoto para el futuro.

La gran mayoría de los encuestados (76 %) consideran que la seguridad y el cumplimiento mejorados son una ventaja principal, lo que refuerza la forma en que zero trust reemplaza el acceso implícito a la red y reduce la exposición al ransomware, el robo de credenciales y los riesgos de movimiento lateral.

Además, el 64 % informa ganancias en simplicidad de gestión, escalabilidad y experiencia del usuario como ventaja principal, ya que zero trust elimina las cargas operativas de administrar concentradores VPN, revisiones constantes y resolución de problemas de acceso.

Cerca de la mitad (45 %) de los encuestados citan el reemplazo de VPN por una solución de zero trust como un paso crítico hacia una arquitectura de 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: mejor experiencia del usuario final (32 %), Integraciones perfectas entre sistemas de TI y seguridad (28 %), y menores costes operativos mediante el ahorro de recursos (18 %). En conjunto, estas ventajas ilustran por qué las organizaciones están eliminando rápidamente las VPN tradicionales en favor de zero trust.

ManpowerGroup, líder mundial en soluciones de personal, ofrece un caso práctico convincente sobre cómo asegurar el acceso con zero trust. Ante la tarea de dar soporte a una gran cantidad de personal remoto, la organización reemplazó con éxito su infraestructura VPN heredada por una solución de zero trust de Zscaler. Sorprendentemente, en tan solo 18 días, ManpowerGroup amplió el acceso seguro a las aplicaciones a más de 30 000 usuarios, logrando una continuidad de negocio ininterrumpida y reduciendo drásticamente las incidencias del soporte técnico en un 97 %. Esta implementación resalta la capacidad de una arquitectura zero trust para escalar rápidamente, simplificar las operaciones e impulsar resultados mensurables para la productividad y la seguridad.

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

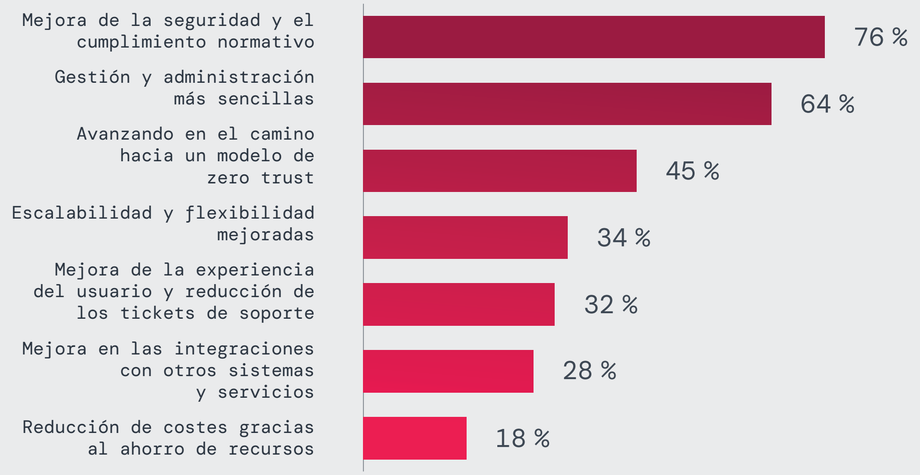


Figura 19: Las empresas comparten las principales ventajas de una solución de zero trust, en comparación con una solución VPN anterior.

La adopción de zero trust debe comenzar con cambios tácticos que eliminen el acceso a la red basado en VPN y favorezcan conexiones directas a nivel de aplicación para contrarrestar los riesgos de movimiento lateral. Las organizaciones pueden priorizar la sustitución del acceso heredado para casos de uso críticos, como la protección de conexiones de usuarios remotos y de terceros, antes de escalar las capacidades de zero trust en 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, a la vez que permiten la escalabilidad en 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 eficiencia.

Predicciones de riesgo de VPN

Seguirán surgiendo vulnerabilidades críticas de VPN

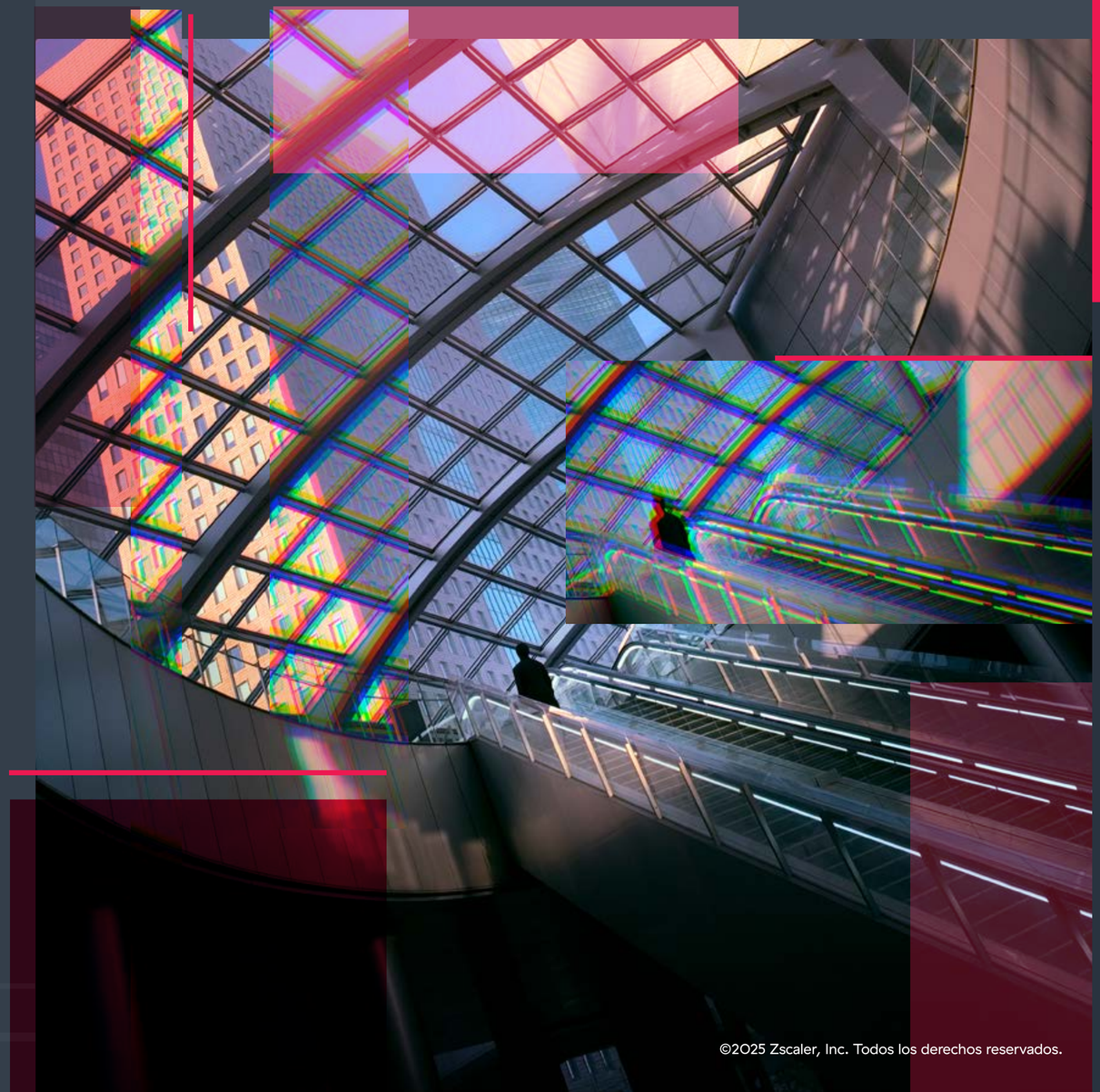
El creciente número de exploits de VPN en los últimos años se acelerará en 2025. Las tecnologías VPN son un objetivo principal para los atacantes porque exponen a las empresas a Internet, lo que hace que las vulnerabilidades sean fáciles de analizar y explotar. A medida que las organizaciones luchan por corregir los fallos de VPN a tiempo, los atacantes continuarán descubriendo y utilizando nuevas vulnerabilidades de alta gravedad, como se vio en el ataque a Ivanti Pulse Secure de enero de 2025. Tanto los investigadores de seguridad como los ciberdelincuentes están investigando activamente las infraestructuras de VPN, lo que hace inevitable la constante divulgación de CVE críticos.

Los grupos de ransomware intensificarán los exploits de VPN

Mientras el 92 % de los encuestados expresan preocupación por las vulnerabilidades de VPN sin revisar, los ciberdelincuentes seguirán explotando fallos de VPN conocidos y de día cero como método principal de acceso inicial. Los grupos de ransomware como servicio (RaaS) frecuentemente buscan VPN expuestas con vulnerabilidades sin revisar, 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 de asistencia sanitaria de EE. UU. demuestra cómo las brechas de seguridad de VPN ofrecen a los atacantes acceso directo a sistemas confidenciales. A medida que estos ataques se vuelvan más automatizados, la necesidad de realizar la transición a una seguridad de zero trust será aún más urgente.

El movimiento lateral a través de VPN provocará ataques más destructivos

Los atacantes aprovechan el amplio acceso que brindan las VPN para moverse lateralmente, escalar privilegios y exfiltrar datos, entre las técnicas más eficaces que utilizan los ciberdelincuentes y los autores de ataques de los estados nacionales. Con un 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 estas dificultades, las empresas deberían adoptar la segmentación de zero trust, que impone un acceso estricto con mínimos privilegios a las aplicaciones, eliminando las vías de movimiento lateral sin la carga operativa de la segmentación de red tradicional.



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

Mientras el 93 % de los encuestados expresan preocupación por las vulnerabilidades de las VPN de terceros, los atacantes seguirán atacando a través de puntos de acceso externos débiles. Las credenciales de terceros robadas y el acceso VPN mal configurado siguen estando entre los principales puntos de entrada de los ciberdelincuentes. La infracción de datos de 2024 de Enterprise Financial Group (EFG) demostró cómo los atacantes explotan las conexiones VPN de terceros para infiltrarse en entornos corporativos. Muchas organizaciones carecen de visibilidad de los permisos de acceso de terceros, lo que dificulta la aplicación de políticas de seguridad. Para mitigar estos riesgos, las organizaciones deben realizar la transición a un marco de zero trust, aplicando un acceso estricto con privilegios mínimos y una verificación continua para todas las conexiones externas.

Los exploits de VPN impulsados por IA aumentarán

El auge de los ciberataques impulsados por IA afectará a la seguridad de las VPN de formas sin precedentes. Los atacantes utilizarán cada vez más la IA para el reconocimiento automatizado, la pulverización inteligente de contraseñas y el desarrollo rápido de vulneraciones, lo que les permitirá comprometer las credenciales de VPN a gran escala. Las técnicas de evasión impulsadas por IA dificultarán aún más la detección de intrusiones basadas en VPN antes de que se produzcan daños significativos. Mientras tanto, las soluciones de seguridad de VPN impulsadas por IA pueden introducir brechas de seguridad imprevistas, lo que generará nuevos vectores de ataque que los ciberdelincuentes explotarán. Ante el aumento de las amenazas impulsadas por IA, las organizaciones deben adoptar medidas de seguridad proactivas, como la verificación continua de identidad y los controles de acceso de zero trust.

Las principales infracciones relacionadas con las VPN serán noticia

Tras múltiples infracciones de alto perfil en 2024, las organizaciones se enfrentarán a una mayor presión para revelar los incidentes cibernéticos relacionados con las VPN. Con las nuevas regulaciones de la SEC que exigen transparencia en los riesgos de ciberseguridad, las organizaciones que sufren vulnerabilidades en sus VPN se enfrentarán a un mayor escrutinio regulatorio, daños a su reputación y posibles sanciones financieras. A medida que las VPN sigan sirviendo como punto de entrada principal para los ataques, las organizaciones se verán obligadas a reevaluar los modelos de acceso tradicionales, lo que acelerará la transición hacia la seguridad de zero trust.

Las inversiones en zero trust aumentarán a medida que las VPN decaigan

Dado que el 65 % de las organizaciones ya están reemplazando o tienen previsto reemplazar sus VPN en el plazo de un año, la inversión en seguridad de zero trust se está acelerando y está transformando fundamentalmente el panorama del acceso remoto. Los requisitos reglamentarios y la obligatoriedad de seguros cibernéticos están impulsando a las organizaciones a ir más allá de las VPN, ya que las soluciones tradicionales no satisfacen las demandas de seguridad, escalabilidad y cumplimiento. La adopción de zero trust no sólo reduce el riesgo cibernético, sino que también elimina los altos costes de mantenimiento de concentradores VPN, dispositivos de red y ciclos continuos de parches. Como resultado, las VPN se consideran cada vez más obsoletas, lo que impulsa un cambio en todo el sector hacia modelos de seguridad de zero trust.

Estas predicciones resaltan un consenso creciente: las organizaciones que retrasen la adopción de 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 revisiones reactivas, por lo que ahora es el momento de ir más allá de las VPN.

Mejores prácticas para un acceso_seguro

Reduzca los riesgos de las VPN y fortalezca la seguridad de zero trust

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

2. **Detenga el ataque inicial con la prevención de amenazas en línea.** Inspeccione todo el tráfico cifrado y no cifrado en línea para bloquear exploits de día cero, malware y cargas útiles de ransomware antes de que lleguen a los usuarios. Puesto que el 92 % de las organizaciones se preocupa por el ransomware que ataca 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 en la nube elimina la necesidad de cortafuegos locales y reduce la superficie de ataque.

3. **Refuerce la autenticación y la seguridad de la identidad.** Implemente la autenticación multifactor (MFA) resistente al phishing, como credenciales FIDO2, biometría o tokens de hardware, para verificar el acceso de los usuarios. Evite los métodos de autenticación tradicionales, como la MFA basada en SMS y las notificaciones push, que los atacantes suelen eludir. Integre seguridad basada en la identidad con verificación continua en lugar de depender de la autenticación única.

4. **Implemente un acceso contextual con privilegios mínimos con ZTNA.** Reemplace el acceso VPN generalizado con acceso a red de zero trust (ZTNA) para garantizar que los usuarios sólo se conecten a las aplicaciones autorizadas, nunca a la red. Los controles de acceso granulares justo a tiempo (JIT) basados en la identidad, la postura del dispositivo y el análisis de riesgos en tiempo real garantizan que los usuarios únicamente puedan acceder a lo que necesitan, cuando lo necesitan.

5. **Elimine el movimiento lateral con la segmentación de zero trust.** Conecte a los usuarios directamente con las aplicaciones, no con la red, para evitar que los atacantes se muevan entre sistemas si obtienen acceso inicial. La segmentación de zero trust y la microsegmentación con reconocimiento de identidad garantizan que, incluso si un usuario se ve comprometido, un atacante no pueda recurrir a otros recursos ni escalar privilegios. ZTNA elimina los túneles VPN, que son un importante facilitador del movimiento lateral.

6. **Proteja el acceso externo y de terceros con controles basados en identidad.** Aplique el acceso con privilegios mínimos a terceros, proveedores y contratistas mediante estrictos controles de sesión, comprobaciones del estado del dispositivo y supervisión continua. Reemplazar el acceso de terceros basado en VPN con ZTNA reduce significativamente la exposición al riesgo de credenciales de proveedores comprometidas, un cambio positivo para el 93 % de las organizaciones preocupadas por los riesgos de las VPN de terceros.

7. **Mejore la protección de datos con políticas de zero trust integradas.** Implemente controles de prevención de pérdida de datos (DLP) y agentes de seguridad de acceso a la nube (CASB) en línea para inspeccionar, cifrar y prevenir la transferencia no autorizada de datos en tiempo real. Un marco de seguridad de zero trust garantiza la inspección y el control de todo el tráfico de usuarios, incluso en aplicaciones SaaS y entornos de nube.

8. **Implemente seguridad basada en IA y supervisión continua.** Utilice análisis basados en IA en tiempo real, tecnología de engaño y detección automatizada de comportamiento para detener las amenazas antes de que se intensifiquen. Las soluciones ZTNA proporcionan calificación de riesgo en tiempo real, lo que impide que las cuentas comprometidas accedan a aplicaciones confidenciales. La búsqueda proactiva diaria de amenazas y los controles de acceso basados en el riesgo reducen significativamente el impacto de las brechas.

9. **Evalúe y adapte continuamente su postura de seguridad.** Realice evaluaciones de riesgos automatizadas, pruebas de penetración y simulaciones de adversarios para ajustar dinámicamente las políticas de seguridad de zero trust. Las configuraciones de seguridad incorrectas y la falta de aplicación son factores clave que contribuyen a brechas de seguridad graves, por lo que la aplicación automatizada y basada en políticas es crucial para reducir el error humano.

10. **Elimine la infraestructura VPN y automatice la aplicación de políticas de seguridad.** Elimine la necesidad de concentradores VPN, administración de reglas de cortafuegos y listas de control de acceso manuales mediante la adopción de un modelo de zero trust en la nube. ZTNA permite políticas de seguridad dinámicas que se adaptan en tiempo real a los cambios de cumplimiento, las actualizaciones regulatorias y la evolución de las ciberamenazas, sin necesidad de configuración manual ni dependencias de hardware.

Al implementar estas mejores prácticas, las organizaciones pueden eliminar los riesgos de seguridad de las VPN con un marco de seguridad de zero trust resistente, que garantiza la verificación continua, el acceso con privilegios mínimos y la mitigación proactiva de amenazas.

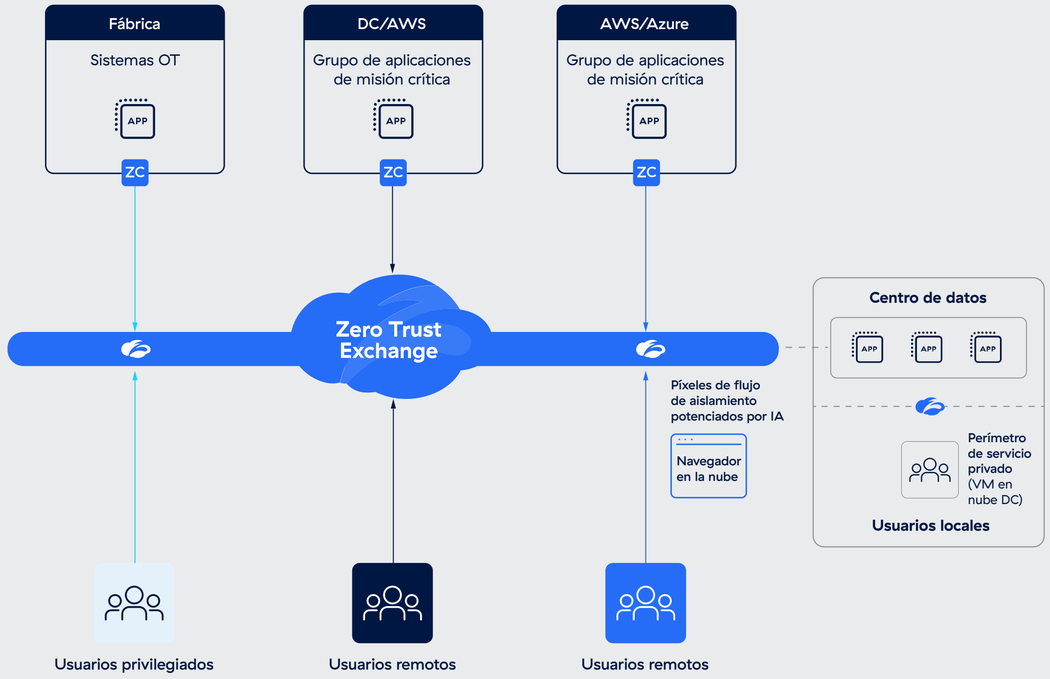
Cómo transforma Zscaler el acceso_seguro

Las VPN y los cortafuegos tradicionales amplían significativamente la superficie de ataque de una organización al colocar a los usuarios directamente en la red. Este amplio acceso facilita que los atacantes exploten vulnerabilidades, accedan y se muevan 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) ofrece una alternativa segura y escalable a las soluciones de acceso remoto tradicionales, como las VPN. Como solución nativa de la nube, ZPA permite el acceso de zero trust para todos los usuarios al ofrecer conectividad directa a aplicaciones privadas. Para minimizar la superficie de ataque, las aplicaciones se protegen tras la plataforma Zscaler Zero Trust Exchange™. Este enfoque elimina el movimiento lateral mediante la segmentación de usuario a aplicación impulsada por IA y protege 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 por una plataforma de zero trust global nativa de la nube. Impulsado por la mayor nube de seguridad 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 del personal distribuido e híbrido en distintas áreas geográficas.

Con ZPA, las empresas pueden adoptar modelos de personal híbrido y centrado 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.



Beneficios clave de Zscaler Private Access (ZPA)

Minimice la superficie de ataque para protegerse contra ataques de ransomware

Las vulnerabilidades de VPN exponen a las organizaciones a usuarios maliciosos, lo que provoca ataques de ransomware y robo de credenciales. ZPA elimina este riesgo ocultando todas las aplicaciones detrás de Zero Trust Exchange y otorgando a los usuarios acceso directo y de zero trust exclusivamente a las aplicaciones autorizadas. Al evitar que usuarios no autorizados, incluidos proveedores y contratistas externos, descubran aplicaciones y se muevan lateralmente, ZPA protege eficazmente frente a 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 en la red. Proporciona información visual sobre el acceso de los usuarios a las aplicaciones y las políticas aplicadas, lo que mejora la visibilidad y el control. La segmentación de ZPA basada en IA genera automáticamente recomendaciones para segmentos y políticas de aplicaciones, simplificando la implementación de la segmentación y garantizando al mismo tiempo 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.

Proporcione acceso sin cliente para mitigar vulnerabilidades de terceros

El acceso sin cliente de ZPA simplifica el acceso de terceros al permitir que contratistas y socios se conecten de forma segura a las aplicaciones a través de cualquier navegador sin necesidad de un cliente. Aísla los dispositivos no administrados de la red corporativa, protege los datos confidenciales y se integra con el navegador Google Chrome Enterprise para una mayor seguridad en casos de uso de dispositivos propios del usuario. Este enfoque moderno reduce costes, minimiza los riesgos asociados al acceso de terceros y elimina la dependencia de la gestión de VDI tradicional.

Prevenga el compromiso de aplicaciones privadas

ZPA minimiza el riesgo de comprometer aplicaciones privadas y la pérdida de datos al realizar una inspección en línea completa del tráfico de aplicaciones privadas de extremo a extremo. Las sólidas capacidades de prevención de pérdida de datos garantizan que la información confidencial permanezca segura al tiempo que bloquean el acceso no autorizado. Al ocultar aplicaciones de Internet público y permitir conexiones seguras entre usuarios y aplicaciones basadas en principios de zero trust, ZPA reduce la superficie de ataque, evita el movimiento lateral y protege contra infracciones, lo que mejora la seguridad general.

Simplifique la gestión de políticas y acelere la implementación

ZPA optimiza las operaciones de TI al simplificar la implementación del acceso remoto, la gestión de políticas y la segmentación de usuarios por aplicación. Tareas que antes consumían mucho tiempo (como la incorporación de usuarios, la aplicación de revisiones y las actualizaciones) ahora se pueden completar en minutos, lo que reduce significativamente la labor 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 control de acceso basado en la postura

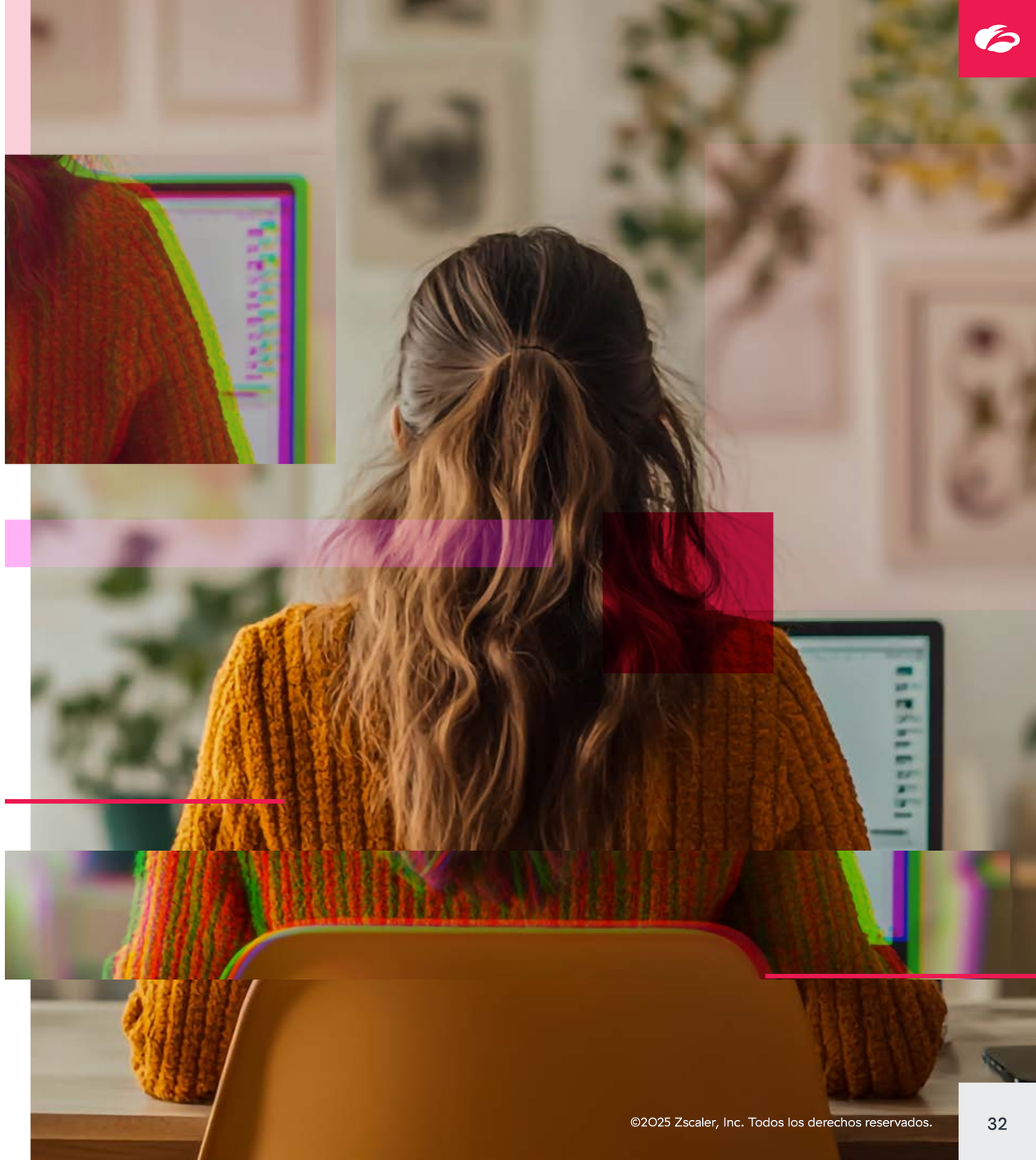
ZPA se integra con herramientas de evaluación de la postura de los terminales para verificar la postura de seguridad de los dispositivos del usuario antes de otorgar acceso. Esto garantiza que únicamente los dispositivos compatibles puedan conectarse, lo que mitiga los riesgos de dispositivos no administrados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

Ofrezca una experiencia de usuario superior

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 retornan tráfico a través de un centro de datos centralizado, ZPA permite conexiones directas de usuario a aplicación a través de Zero Trust Exchange. Esto reduce drásticamente la latencia y mejora el rendimiento de la aplicación, tanto si los usuarios trabajan localmente, de forma remota o se encuentran de viaje. 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 proactiva de ZPA agilizan la resolución de problemas, garantizando un acceso ininterrumpido y de alta calidad para todos los usuarios.

Reduzca el coste total de propiedad

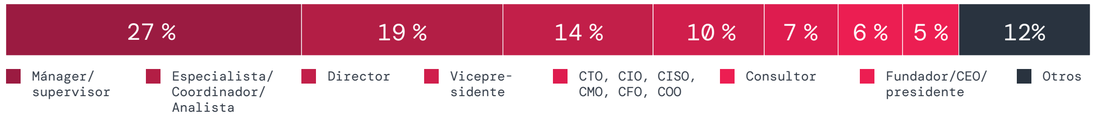
ZPA reduce significativamente el costo total de propiedad al eliminar la necesidad de múltiples productos puntuales, como VPN, cortafuegos, NAC y concentradores VPN. Construido sobre una arquitectura de zero trust nativa de la nube, ZPA elimina los costes de infraestructura relacionados con el soporte 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.



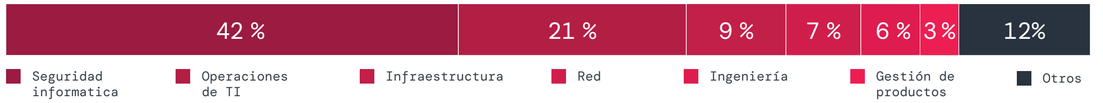
Metodología_y datos demográficos

Este informe se basa en una encuesta exhaustiva a 632 profesionales de TI y ciberseguridad realizada a principios de 2025, que examinó los riesgos de seguridad de VPN, las tendencias de acceso empresarial y la adopción de arquitecturas de zero trust. Entre los encuestados se encontraban ejecutivos, profesionales de seguridad informática y líderes de infraestructura de red de diversos sectores. Los hallazgos de este informe brindan una perspectiva basada en datos sobre el declive de las VPN y el cambio hacia zero trust, ofreciendo información fundamental para las organizaciones que modernizan sus estrategias de seguridad de acceso.

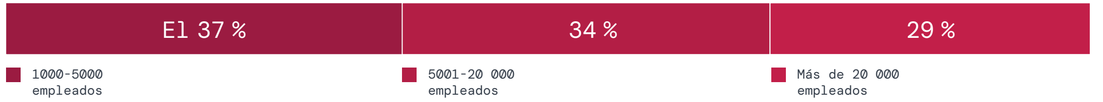
Nivel profesional



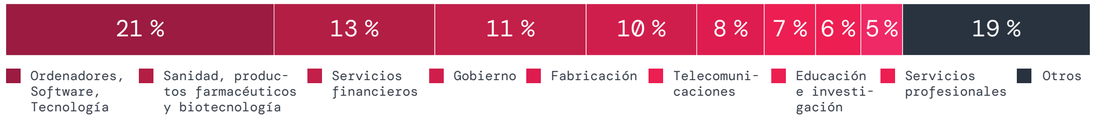
Departamento



Tamaño de la empresa



Sector



Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite **www.zscaler.com/es.**

Acerca de ThreatLabz

ThreatLabZ es la división de investigación de seguridad de Zscaler. Este equipo de primera clase es responsable de buscar nuevas amenazas y garantizar que las miles de organizaciones que usan la plataforma global Zscaler estén siempre protegidas. Además de investigar el malware y de analizar los comportamientos, los miembros del equipo participan en la investigación y el desarrollo de nuevos módulos prototipo para la protección avanzada contra las amenazas en la plataforma Zscaler. Asimismo, realizan habitualmente auditorías de seguridad internas para garantizar que los productos y la infraestructura de Zscaler satisfacen los estándares de cumplimiento 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 CONFIABLE DE INFORMACIÓN SOBRE CIBERSEGURIDAD BASADA EN DATOS

Cybersecurity Insiders ofrece información respaldada por evidencia y validación de terceros, lo que permite a los líderes en ciberseguridad tomar decisiones estratégicas informadas. Con más de una década de investigación a sus espaldas y una red global de más de 600 000 profesionales de la ciberseguridad, ofrecemos inteligencia práctica que ayuda a los líderes a afrontar amenazas en constante evolución, evaluar nuevas tecnologías y diseñar estrategias prospectivas con confianza.

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

Al combinar este contenido con una distribución integrada, ayudamos a las marcas a ganar confianza, aumentar el conocimiento e impulsar la demanda en un mercado de ciberseguridad abarrotado.

Más información: cybersecurity-insiders.com

Holger Schulze,
director ejecutivo y fundador
de Cybersecurity Insiders

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 de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo , Zero Trust Exchange™ basada en SSE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite **www.zscaler.com/es** o síganos en Twitter**@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/es**