Informe de riesgos de las VPN de Zscaler ThreatLabz 2024

Cybersecurity INSIDERS

Explore las tendencias clave en materia de seguridad, riesgo y experiencia de usuario de las VPN, a medida que la adopción de Zero Trust alcanza un impulso crítico.

Contenido

Información general

El actual entorno de trabajo distribuido y centrado en la nube ha provocado un cambio en los métodos de acceso, que han pasado de las tradicionales redes privadas virtuales (VPN) a marcos de seguridad más robustos como Zero Trust. Tradicionalmente, las VPN proporcionaban capacidades esenciales de acceso remoto para conectar usuarios o sitios de oficina enteros. Sin embargo, la creciente sofisticación de las ciberamenazas junto con la expansión de las fuerzas de trabajo remotas y las tecnologías en la nube han expuesto vulnerabilidades significativas en las VPN. Debido a su arquitectura heredada, las VPN conceden un acceso demasiado amplio a la red una vez que se verifican las credenciales, lo que aumenta significativamente el riesgo de ciberataques si dichas credenciales se ven comprometidas.

Los recientes exploits de alto perfil de los dispositivos VPN han puesto de manifiesto vulnerabilidades críticas (en particular CVE-2023-46805, CVE-2024-21887 y CVE-2024-21893) que afectan a sectores esenciales, incluida la defensa estadounidense. Estas vulnerabilidades permiten a los atacantes eludir la autenticación, ejecutar comandos con privilegios elevados y mantener la persistencia después de reiniciar el dispositivo. Ante esta situación, la Agencia de Ciberseguridad y Seguridad de las Infraestructuras de los Estados Unidos (CISA) emitió una directiva de emergencia a las agencias federales para que desconectaran inmediatamente los dispositivos VPN afectados debido a los importantes riesgos de seguridad.

A través del Decreto 14028, el gobierno de los EE. UU. exige ahora la adopción de arquitecturas Zero Trust para mejorar la ciberseguridad, alejándose de las redes privadas virtuales tradicionales. Esta directiva, que forma parte de una estrategia global para reforzar la ciberseguridad nacional, ordena a las agencias federales que apliquen Zero Trust, que verifica cada solicitud de acceso independientemente de su origen. La Oficina de Gestión y Presupuesto (OMB, por sus siglas en inglés) apoya además esta iniciativa con una detallada Estrategia Federal de Zero Trust, que destaca el cambio de una confianza implícita basada en VPN dentro de los perímetros de la red a una verificación continua de todas y cada una de las solicitudes de acceso. Estas directivas y recomendaciones reflejan un consenso dentro de la comunidad de la ciberseguridad en el sentido de que Zero Trust ofrece una defensa más sólida contra las ciberamenazas complejas y en evolución, una necesidad acentuada por las recientes vulnerabilidades y exploits relacionados con las VPN tradicionales.

En consecuencia, las organizaciones están adoptando rápidamente modelos Zero Trust, que no confían intrínsecamente en ningún usuario o dispositivo dentro o fuera del perímetro de la red y exigen una verificación granular para cada solicitud de acceso. Este modelo es especialmente eficaz para impedir el movimiento lateral dentro de las redes, un exploit que los atacantes suelen utilizar para profundizar en su intrusión tras obtener el acceso inicial.

Basado en una encuesta realizada a 647 profesionales de TI y expertos en ciberseguridad, este informe explora los variados desafíos de seguridad y experiencia de usuario de las VPN para poner de manifiesto la complejidad de la gestión actual del acceso, las vulnerabilidades ante diversos ciberataques y su potencial para perjudicar la postura de seguridad más amplia de las organizaciones. El informe también esboza modelos de seguridad más avanzados, en particular el de Zero Trust, que se ha establecido firmemente como un marco sólido y orientado al futuro para asegurar y acelerar la transformación digital.

Agradecemos a Zscaler por contribuir a esta encuesta de riesgo de las VPN. Su experiencia en soluciones de acceso seguro y Zero Trust ha enriquecido significativamente nuestros hallazgos. Creemos firmemente que las ideas de este informe serán un recurso esencial para los profesionales de TI y ciberseguridad en su camino hacia la seguridad Zero Trust.

Gracias,
Holger Schulze, fundador de Cybersecurity Insiders

"En el último año, numerosas vulnerabilidades críticas de las VPN han servido como puntos de entrada importantes para ataques a grandes empresas y entidades federales. Teniendo en cuenta estos resultados repetidos, es crucial que las empresas prevean que los malintencionados explotarán cada vez más estos activos heredados y expuestos a Internet (dispositivos y virtuales) que les permiten navegar lateralmente con facilidad a través de las redes planas tradicionales. La transición a una arquitectura Zero Trust es esencial, ya que reduce significativamente la superficie de ataque al eliminar las tecnologías heredadas como las VPN y los firewalls, impone controles de seguridad uniformes con la inspección TLS y limita el radio de explosión con la segmentación y el engaño, lo que evita violaciones perjudiciales."

—DEEPEN DESAI, DIRECTOR DE SEGURIDAD DE ZSCALER

Hallazgos clave

Los ataques a las VPN van en aumento.

El 56 % de las organizaciones sufrieron uno o más ciberataques relacionados con las VPN en el último año (frente al 45 % del año anterior), lo que pone de manifiesto la creciente frecuencia y sofisticación de los ataques dirigidos contra las VPN.

Las VPN no son rival para ransomware, malware y DDoS.

Los encuestados identificaron el ransomware (42 %), el malware (35 %) y los ataques DDoS (30 %) como las principales amenazas que aprovechan las vulnerabilidades de las VPN, lo que pone de relieve la amplitud de los riesgos a los que se enfrentan las organizaciones debido a las debilidades inherentes a las arquitecturas VPN tradicionales.

La gran mayoría se está pasando a Zero Trust.

El 78 % de las organizaciones planea implementar estrategias Zero Trust en los próximos 12 meses. Mientras tanto, el 62 % de las empresas está de acuerdo en que las VPN son anti-Zero Trust.

El riesgo de movimiento lateral no puede ignorarse.

El 53 % de las empresas violadas a través de vulnerabilidades de VPN afirman que los malintencionados se desplazaron lateralmente, lo que demuestra fallas de contención en el punto inicial de compromiso que subrayan los riesgos de las redes planas tradicionales.

La mayoría tiene dudas sobre la seguridad de las VPN.

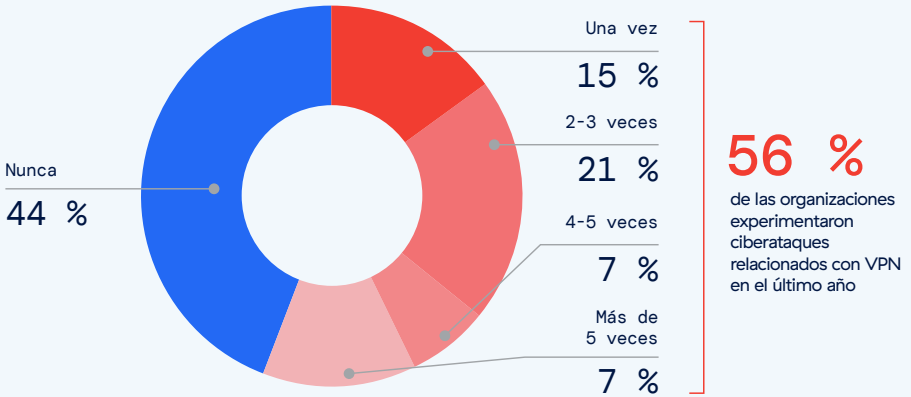
El 91 % de los encuestados expresaron su preocupación por que las VPN comprometan su entorno de seguridad informática, y las recientes violaciones ilustran los riesgos que supone mantener infraestructuras de VPN anticuadas o sin parches.

Cuestiones de seguridad con VPN

Los ataques a las VPN van en aumento

La frecuencia y la gravedad de los ataques que aprovechan las vulnerabilidades de las VPN ponen de manifiesto la ineficacia de las medidas de ciberseguridad convencionales y subrayan los riesgos persistentes que plantea la exposición de las redes. Nuestra encuesta revela que el 56 % de las organizaciones sufrieron ciberataques el año pasado en los que se aprovecharon las vulnerabilidades de las VPN, un aumento significativo respecto al 45 % del año anterior. Resulta alarmante que el 41 % de las organizaciones declararan haber sufrido dos o más ataques relacionados con las VPN, lo que indica graves deficiencias en la seguridad.

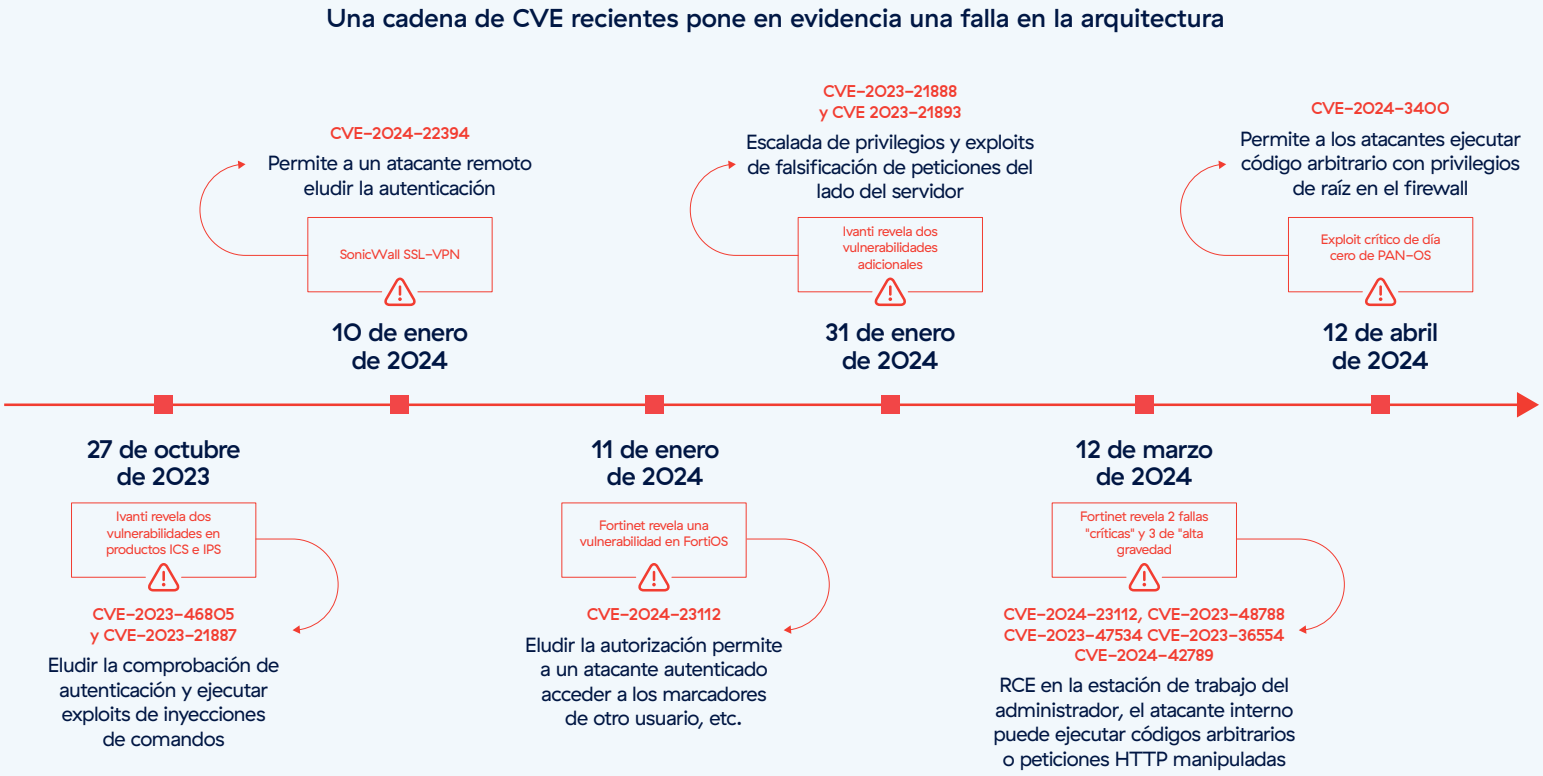
En los últimos 12 meses, ¿con qué frecuencia ha sufrido su organización un ataque que se aprovechara de las vulnerabilidades de seguridad de sus servidores VPN?



Las últimas tendencias confirman que los ataques a las VPN no solo son cada vez más frecuentes, sino también más sofisticados. Por ejemplo, el aumento de los casos de ransomware que aprovechan las fallas de las VPN (sobre todo a raíz de las vulnerabilidades divulgadas públicamente) pone de manifiesto las debilidades críticas inherentes a las VPN tradicionales. Estas vulnerabilidades ofrecen a los atacantes puntos de entrada fáciles para infiltrarse en las redes y facilitar el movimiento lateral, lo que conduce a importantes violaciones de datos e interrupciones operativas.

Vulnerabilidades importantes de VPN en el último año

En medio de la reciente cadena de CVE de alta gravedad que afectan a los productos VPN, no es de extrañar que las empresas estén reportando más ataques que explotan este tipo de vulnerabilidades. Por supuesto, ningún proveedor ni ninguna tecnología en particular puede ser inmune a las vulnerabilidades del software. En el caso de las VPN, el desafío para las empresas es que cada CVE puede representar un único punto de falla de seguridad para la empresa: un punto de apoyo que permite a los atacantes comprometer un activo VPN, establecer su persistencia, desplazarse lateralmente por la red y robar datos. Como las CVE de VPN siguen divulgándose a este ritmo, serán un riesgo persistente para las empresas que utilizan VPN para la conectividad remota.



Navegar por las cuestiones de seguridad de las VPN

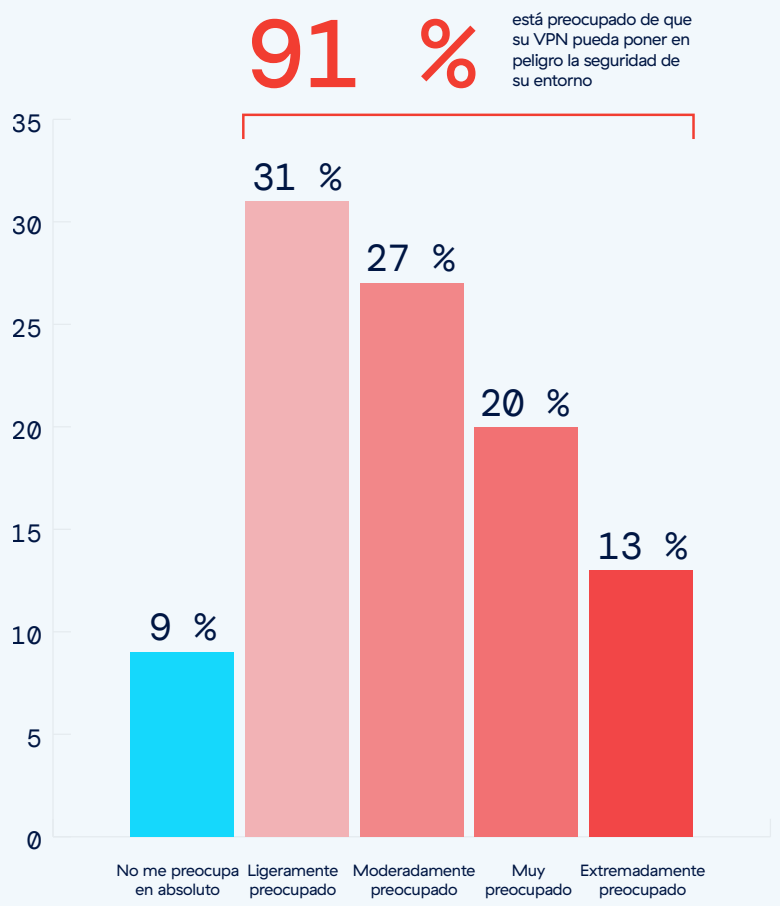
Los resultados de la encuesta reflejan cuestiones muy extendidas sobre las VPN que comprometen los entornos de seguridad, haciendo eco de las tendencias actuales y de las crecientes vulnerabilidades de las tecnologías VPN. Una aplastante mayoría de los encuestados (91 %, frente al 88 % en 2023) manifiesta su preocupación por que las VPN pongan en peligro su seguridad informática, lo que demuestra una mayor sensibilización de las organizaciones ante los riesgos relacionados con las VPN.

Esta preocupación está justificada por los recientes exploits dirigidos a las VPN de Ivanti, en los que los atacantes aprovecharon vulnerabilidades graves para infiltrarse en las redes y exfiltrar datos confidenciales. Estos incidentes, relacionados con vulnerabilidades como CVE-2024-21888 y CVE-2024-21893, ponen de relieve los riesgos de mantener y blindar infraestructuras VPN anticuadas o sin parches. Además, la arquitectura inherente de las VPN plantea importantes riesgos de seguridad en el actual panorama digital sin perímetros. A medida que las empresas adoptan cada vez más servicios en la nube y evolucionan los modelos de trabajo a distancia, las VPN se enfrentan a nuevos desafíos de seguridad, como la gestión de un gran número de derechos de acceso y la protección de una superficie de ataque cada vez mayor.

Estas vulnerabilidades y limitaciones de la arquitectura evidencian un cambio fundamental en la percepción de la seguridad de las VPN, en consonancia con tendencias más amplias de ciberseguridad que abogan por marcos más dinámicos y resistentes, como Zero Trust.

Las organizaciones con visión a largo plazo realizan la transición hacia arquitecturas Zero Trust para obtener un control más granular y reducir significativamente la superficie de ataque al no conferir nunca una confianza implícita, ya sea dentro o fuera del perímetro de una red. La adopción de una estrategia de este tipo aborda las vulnerabilidades inmediatas de las VPN tradicionales y se alinea con un enfoque proactivo de la ciberseguridad, esencial para adaptarse al cambiante panorama de las amenazas.

¿Cuánto le preocupa que la VPN pueda poner en peligro la capacidad de mantener la seguridad de sus entornos informáticos?

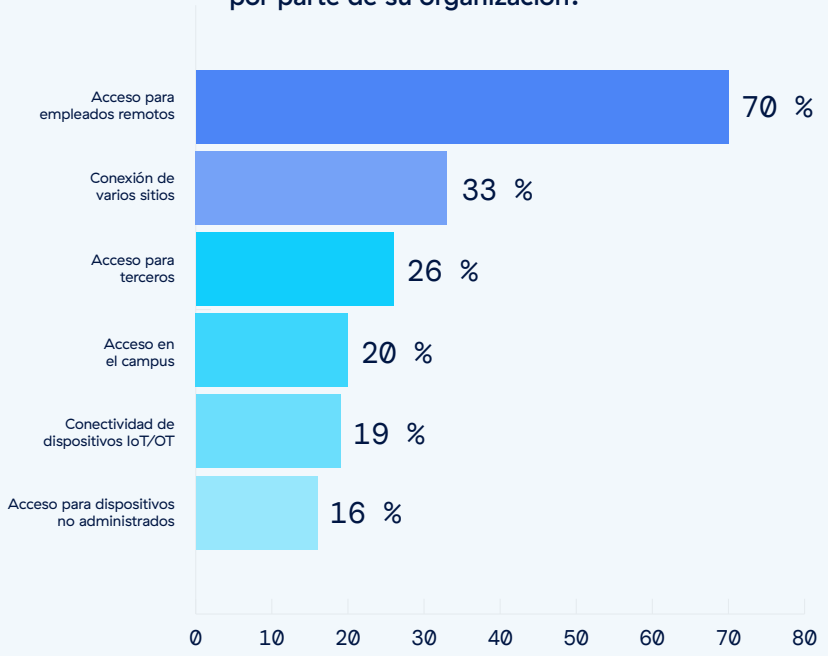


Escenarios clave para un acceso seguro

Comprender por qué las organizaciones utilizan VPN es clave, ya que resalta cómo priorizan el acceso seguro en diversos escenarios comerciales. También revela qué casos de uso de las redes están más expuestos a los riesgos de seguridad, indicando las áreas que requieren estrategias de seguridad de acceso más sólidas e innovadoras.

Un considerable 70 % de las organizaciones utilizan las VPN principalmente para asegurar el acceso de los empleados remotos. Este uso generalizado hace que el acceso remoto sea un blanco principal para los ciberataques. Seguidamente, el 33 % utiliza VPN para conectar varios sitios, lo que presenta riesgos sustanciales, ya que estas conexiones pueden servir de vectores para ciberataques si no están debidamente protegidas. A su vez, el 26 % de las organizaciones observó el acceso de terceros, lo que complica aún más la seguridad debido a las diferentes posturas de seguridad de las distintas partes interesadas externas y a la falta de control sobre las políticas de seguridad. Además, el 20 % de las organizaciones utilizan VPN para el acceso dentro del campus y el 19 % para la conectividad de dispositivos IoT/OT.

¿Cuál es el objetivo principal del uso de las VPN por parte de su organización?



Las VPN ya no brindan la seguridad adecuada para los casos de uso de acceso crítico en el cambiante panorama actual de las ciberamenazas porque funcionan con modelos de confianza obsoletos que conceden un amplio acceso a la red con una simple autenticación del usuario. Este amplio acceso expone a las organizaciones a riesgos significativos al permitir a los atacantes potenciales explotar un único punto de entrada para navegar y extraer datos confidenciales a través de la red.

Gestión, rendimiento y experiencia de usuario de VPN

Desafíos en la gestión de VPN

Además de los riesgos de seguridad inherentes, la gestión de las infraestructuras VPN presenta importantes desafíos para los equipos de TI a medida que se intensifican los requisitos de soluciones de acceso robustas en entornos de trabajo dispersos y centrados en la nube. El principal desafío en materia de gestión para los profesionales de TI es el equilibrio entre el rendimiento de la VPN y la experiencia del usuario (19 %). Este tema es crucial porque repercute directamente en la productividad: si la VPN ralentiza la red o resulta demasiado complicada de utilizar, puede dar lugar a una menor satisfacción de los empleados y a procesos empresariales lentos e ineficaces.

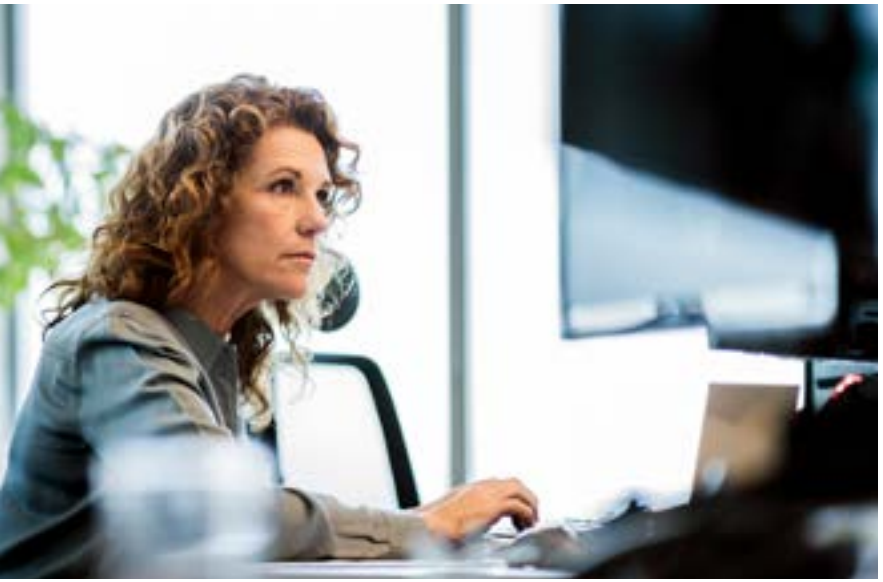
La siguiente preocupación más común, citada por el 17 % de los encuestados, es la resolución constante de problemas de conectividad y estabilidad de la VPN. Estos problemas no solo suponen una pérdida de tiempo para el equipo de TI, sino que también provocan interrupciones molestas para los usuarios. Otros desafíos notables son la falta de compatibilidad de las VPN con una amplia gama de dispositivos, sistemas operativos y aplicaciones, que cerca del 16 % de los profesionales de TI consideran una carga. Además, el 13 % de los encuestados se enfrentan a la complejidad y la laboriosidad de ampliar la infraestructura VPN, un problema crítico a medida que las organizaciones crecen y sus necesidades aumentan en medio de una grave escasez de profesionales cualificados en ciberseguridad.

Estos datos subrayan la necesidad de que las organizaciones exploren alternativas más ágiles, fáciles de usar y que requieran menos recursos, como los modelos de acceso a la red Zero Trust (ZTNA). La ZTNA ofrece un control más granular, una mayor escalabilidad y una menor sobrecarga de gestión, lo que la convierte en una opción superior a la VPN tradicional en el dinámico panorama actual de la ciberseguridad.

Desafíos comunes de los usuarios de VPN

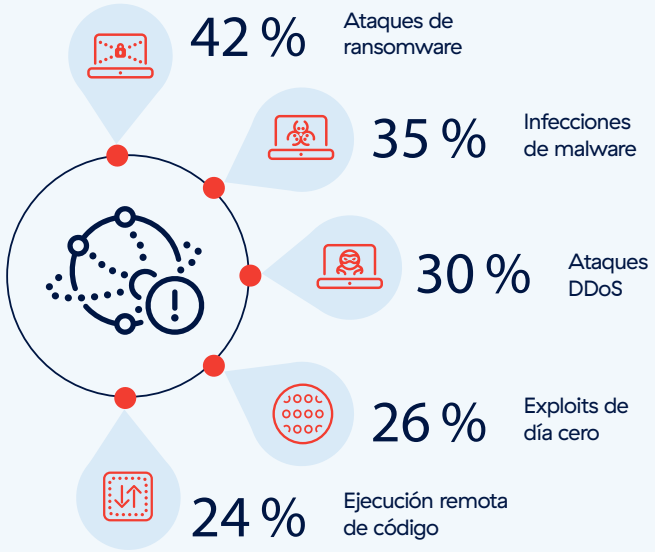
La queja más frecuente de los usuarios sobre el uso de las VPN, señalada por el 26 % de los encuestados, es la lentitud de la velocidad de conexión. Esto pone de relieve un problema crítico de productividad y satisfacción de los usuarios, ya que las velocidades lentas pueden reducir significativamente la eficacia de las tareas rutinarias y el acceso a los recursos basados en la nube, especialmente en entornos de trabajo desde casa.

Las caídas de la conexión a las VPN representan el segundo problema más común, citado por el 19 % de los encuestados. Este problema puede interrumpir las tareas y comunicaciones en curso, afectando significativamente a la experiencia del usuario y a la continuidad operativa. Las experiencias de usuario inconsistentes en diferentes dispositivos y plataformas, señaladas por el 12 % de los usuarios, apuntan a la necesidad de un rendimiento de acceso más uniforme.



Para hacer frente a estas cuestiones, las organizaciones deben considerar la adopción de soluciones de acceso a la red que ofrezcan más estabilidad y uniformidad entre las distintas plataformas. La implementación de una arquitectura Zero Trust puede ser especialmente eficaz, ya que mejora la seguridad sin crear cuellos de botella en el rendimiento Las redes Zero Trust garantizan que los problemas de conexión no comprometan la seguridad y que el control de acceso sea a la vez estricto y adaptable a los distintos entornos de usuarios.

¿Qué tipos de ciberataques cree que tienen más probabilidades de explotar las vulnerabilidades de la VPN de su organización?



Para contrarrestar estas vulnerabilidades, las organizaciones deben adoptar medidas de seguridad proactivas como un modelo Zero Trust. Zero Trust aplica estrictos controles de acceso y una verificación continua de todas las conexiones de red, independientemente de su origen. Esta estrategia mitiga eficazmente los riesgos planteados por una amplia gama de ataques que aprovechan los puntos débiles de las VPN, limitando el movimiento lateral y reforzando los controles de acceso robustos.

Exploits de vulnerabilidad de VPN

La variedad de ciberataques que aprovechan las debilidades de las VPN pone de relieve la magnitud de los riesgos a los que se enfrentan las organizaciones. La encuesta revela que el 42 % de los encuestados identifica los ataques de ransomware como los más propensos a explotar las vulnerabilidades de las VPN, lo que pone de manifiesto su impacto considerable y su frecuencia. Le siguen las infecciones por malware, señaladas por el 35 % de los encuestados, y los ataques DDoS (señalados por el 30 %) que comprometen tanto la disponibilidad como la confidencialidad e integridad de los sistemas.

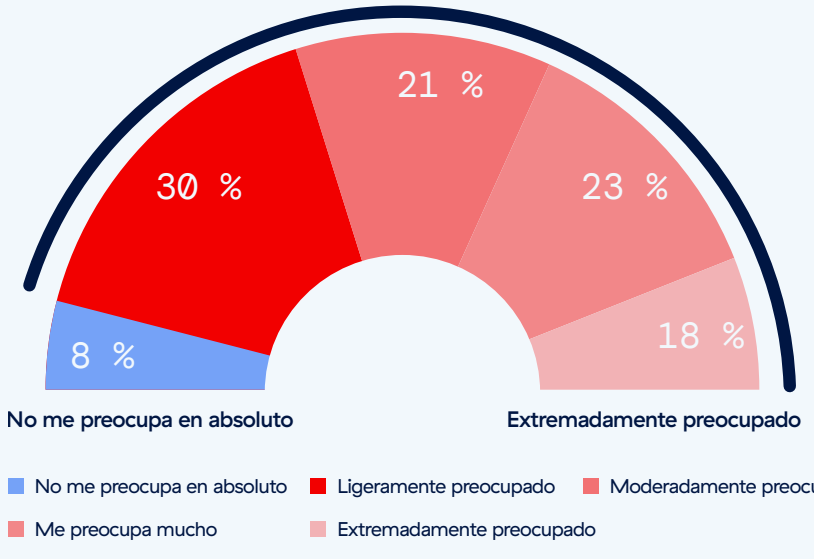
Riesgo de VPN de terceros

La encuesta destaca una preocupación importante en torno al acceso a VPN de terceros como vulnerabilidad de la seguridad de la red. El 92 % de los encuestados expresan su temor ante este riesgo, lo que supone un ligero aumento con respecto al 90 % de 2023. Esta tendencia en alza pone de relieve la posibilidad de acceso de terceros como punto de entrada para las ciberamenazas.

Los nuevos conocimientos sobre las vulnerabilidades y las violaciones de las VPN han validado aún más estas cuestiones. Las VPN tradicionales suelen proporcionar un acceso extenso a la red tras la validación de las credenciales, lo que plantea riesgos si las medidas de seguridad de terceros proveedores se ven comprometidas.

¿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?

92 % les preocupa que entidades externas sirvan como posibles puertas traseras a sus redes a través del acceso VPN



Las organizaciones deberían acelerar su transición de las VPN tradicionales a las arquitecturas Zero Trust. Este cambio implica implementar sistemas que verifiquen rigurosamente las solicitudes de acceso en función de la identidad y el contexto, limitando a los proveedores externos a los recursos específicos esenciales para sus tareas.

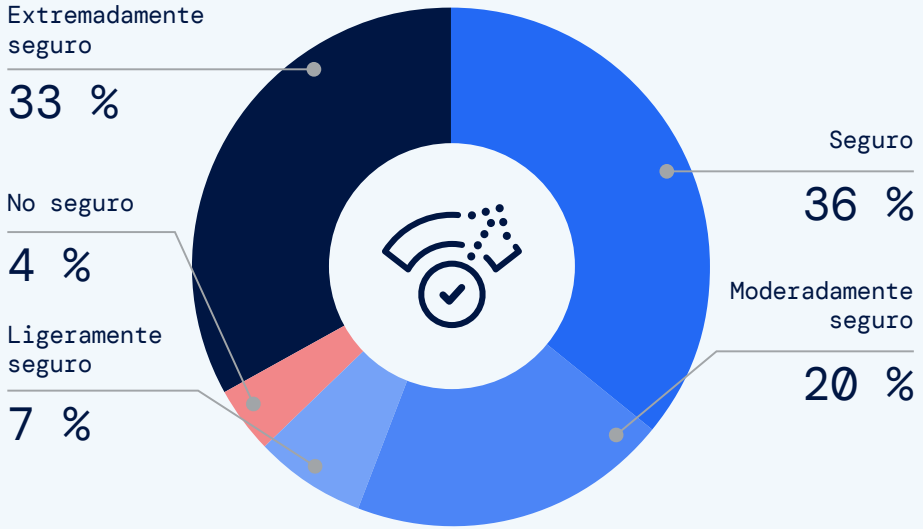
Problemas de seguridad con la infraestructura VPN

Exceso de confianza en la seguridad de VPN

El reciente aumento de las violaciones de las VPN evidencia una desconexión entre la seguridad percibida y el riesgo real. Los recientes exploits de alta gravedad en productos VPN demuestran que incluso las organizaciones bien preparadas podrían estar subestimando las capacidades de los ciberadversarios que explotan las vulnerabilidades inherentes a la tecnología VPN. Un importante 69 % de los encuestados se mostró muy convencido de la capacidad de su organización para hacer frente a las vulnerabilidades de las redes privadas virtuales (VPN), lo que puede no corresponderse del todo con el creciente panorama de las amenazas, en el que actores sofisticados explotan incluso las pequeñas debilidades con gran rapidez. El exceso de confianza puede ser especialmente peligroso dada la complejidad y persistencia de los recientes exploits de VPN, como demuestran los incidentes protagonizados por grupos patrocinados por el Estado y bandas de ciberdelincuentes que atacan sistemas sin parches durante períodos prolongados.

Las organizaciones deben recalibrar su postura de seguridad incorporando evaluaciones rigurosas de las vulnerabilidades, actualizaciones frecuentes y una formación exhaustiva de sensibilización en materia de seguridad. Es aconsejable adoptar un enfoque de seguridad por capas que no dependa excesivamente de las VPN para una protección completa. Este enfoque debe incluir supervisión avanzada, detección de anomalías e integración de principios Zero Trust.

¿Qué confianza tiene en la capacidad de su organización para detectar y mitigar las vulnerabilidades de VPN que la exponen a ataques de ciberseguridad?

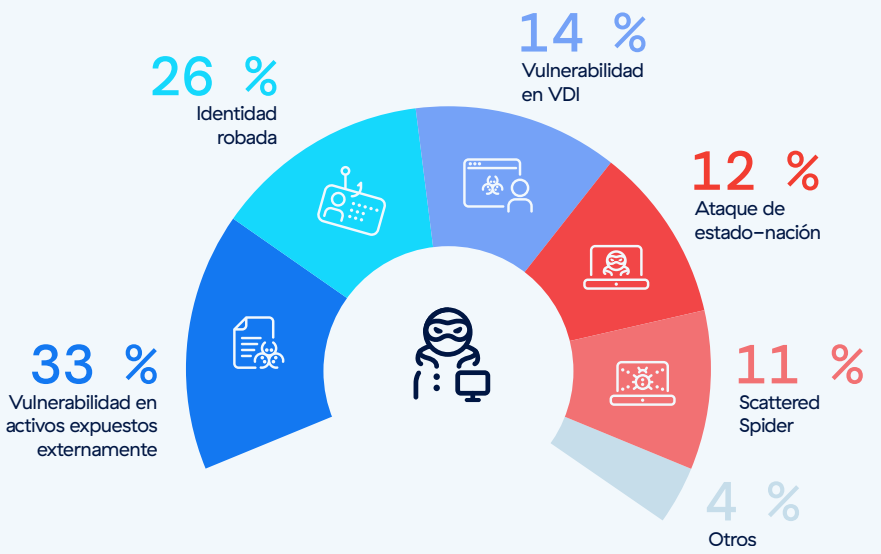


Vectores de ataque de ransomware

La encuesta identifica claramente las vulnerabilidades en los activos expuestos externamente como el vector de ataque potencial del ransomware más preocupante, señalado por el 33 % de los encuestados. Esto indica una aceptación generalizada de los riesgos asociados a los servicios de red o aplicaciones web expuestos, que suelen ser el primer punto de entrada de los ataques de ransomware.

Las identidades robadas le siguen de cerca con un 26 %, lo que subraya la importancia de las credenciales comprometidas al permitir a los atacantes eludir las medidas de seguridad y obtener acceso para enviar cargas útiles de ransomware. La preocupación por las vulnerabilidades de las infraestructuras de escritorios virtuales (VDI) y los ataques de estados-nación, con un 14 % y un 12 % respectivamente, ponen de relieve los diversos orígenes de las amenazas de ransomware contra las que deben defenderse las organizaciones. Scattered Spider (un grupo de ciberdelincuentes que utiliza sofisticadas tácticas de ingeniería social, como el phishing, los ataques de fatiga por autenticación multifactor y el intercambio de SIM), preocupa al 11 % de los participantes.

¿Qué es lo que más le preocupa como causa principal del ransomware?



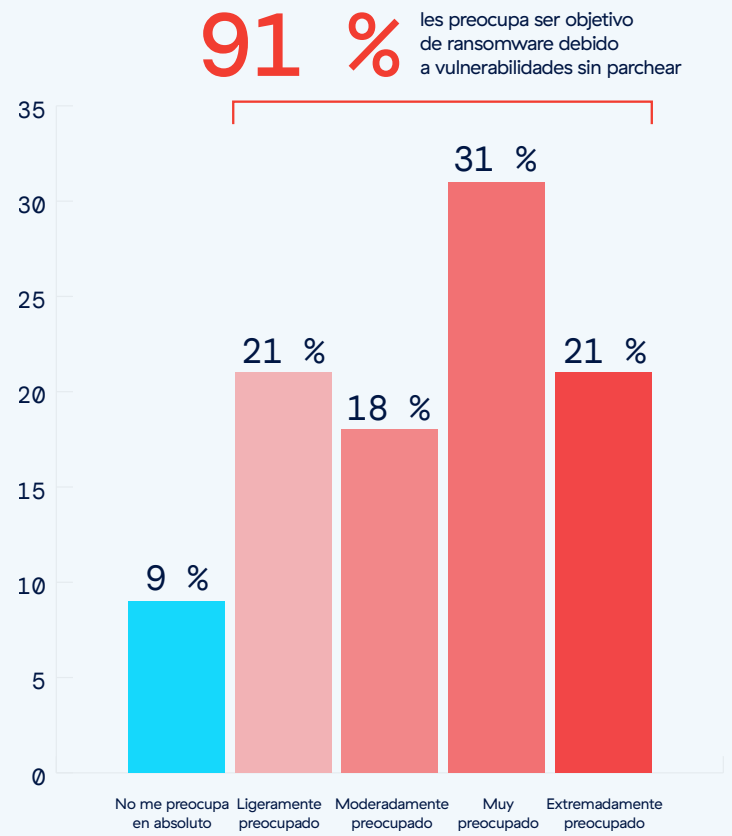
Las organizaciones deben mejorar sus defensas y protocolos de gestión de identidades. La aplicación de procesos exhaustivos de gestión de vulnerabilidades y la adopción de un modelo de seguridad Zero Trust pueden reducir eficazmente el riesgo de ataques de ransomware al denegar el acceso a los recursos de la red y la propagación lateral.

Cuestiones sobre ransomware

Los resultados de la encuesta muestran que el 52 % de los encuestados están muy o extremadamente preocupados por la amenaza del ransomware debido a vulnerabilidades no parcheadas. Esto se justifica por el hecho de que las vulnerabilidades no parcheadas siguen siendo un vector de ataque primario para el ransomware. Análisis recientes muestran que una parte sustancial de los ataques de ransomware aprovechan estas vulnerabilidades, con un impacto notablemente grave en comparación con otros tipos de ciberataques.

Los grupos de ransomware son cada vez más sofisticados, y muchos utilizan ahora tácticas avanzadas que pueden explotar rápidamente vulnerabilidades recién descubiertas antes de que las organizaciones puedan parchearlas. Este acelerado ciclo de explotación acorta enormemente la ventana de respuesta a las vulnerabilidades críticas, lo que subraya la urgente necesidad de medidas de seguridad avanzadas que reduzcan la superficie de ataque.

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



Movimiento lateral en ataques a las VPN

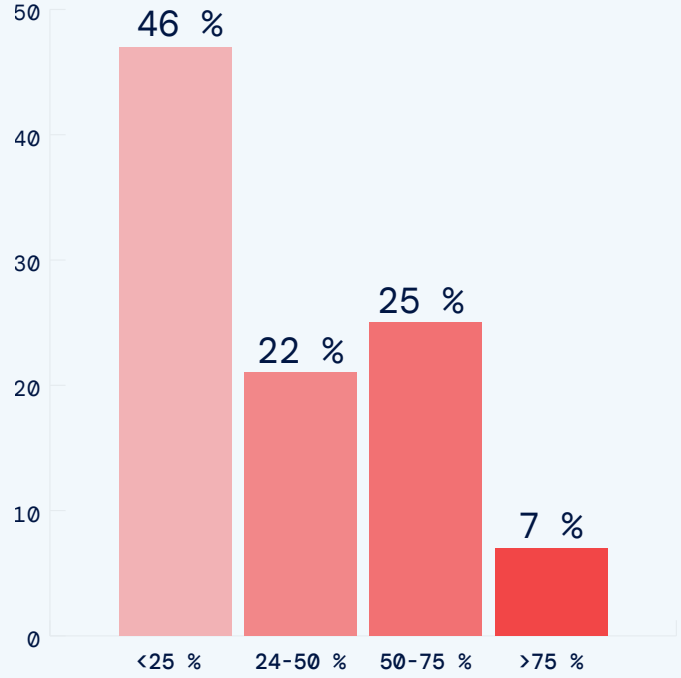
La mayoría de los encuestados (53 %) informan de que más del 25 % de los ataques relacionados con VPN se realizaron mediante movimiento lateral, lo que demuestra fallas significativas de contención en el punto inicial de compromiso. Casi un tercio (32 %) sufrió movimientos laterales en más de la mitad de los ataques, lo que indica importantes desafíos a la hora de controlar la propagación de las amenazas una vez que los adversarios traspasan las defensas de la red.

El movimiento lateral es un riesgo importante para las VPN, ya que los atacantes pueden conseguir un acceso muy amplio a la red, similar al de un usuario autenticado. Esto les permite moverse sigilosamente por la red y apuntar a zonas confidenciales.

De este modo, las VPN pueden agravar los riesgos y ampliar el alcance de un ataque más allá de su punto de entrada inicial. Para resolver esto se necesita una segmentación estricta, idealmente con tráfico de usuario a aplicación a través de una arquitectura Zero Trust, y una supervisión continua. Esto reduce sustancialmente el radio de movimiento lateral de la explosión al permitir el acceso granular a un conjunto más pequeño de aplicaciones para cada usuario individual, mientras que el resto se vuelve invisible.

La creciente sofisticación de los ataques que aprovechan las vulnerabilidades de las VPN subraya la necesidad de un cambio hacia un marco Zero Trust. Al aplicar estrictos controles de acceso y una verificación continua, Zero Trust limita los movimientos laterales no autorizados y mejora la seguridad en los entornos digitales en expansión.

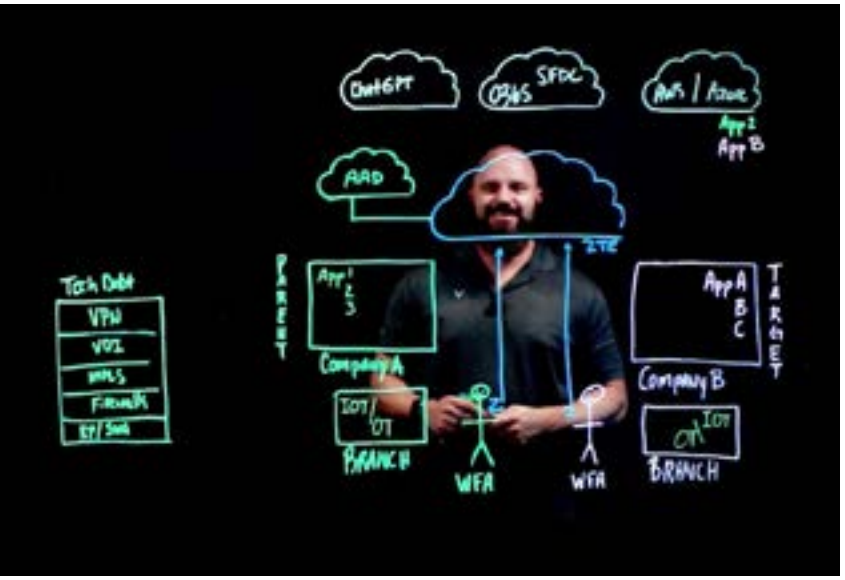
De todos los ataques que ha sufrido su organización, ¿qué porcentaje consistió en amenazas que se propagaron lateralmente tras obtener acceso a través de una VPN?



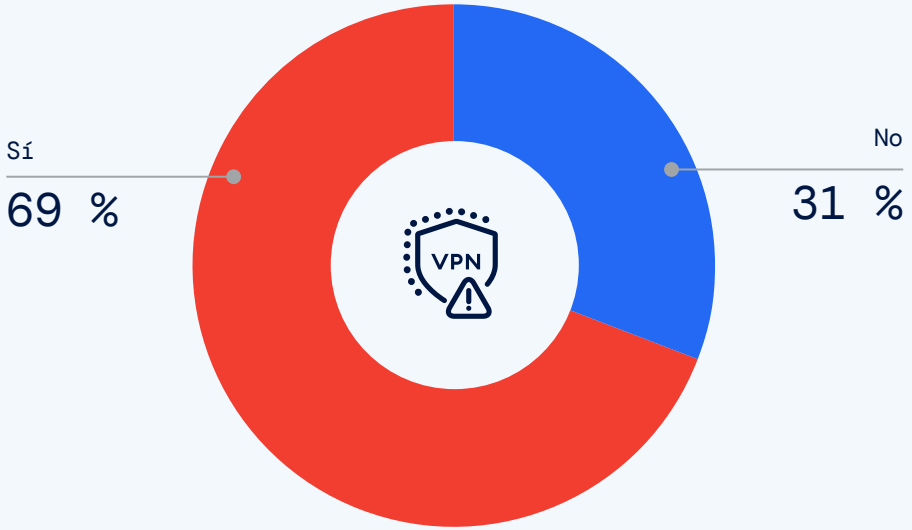
Cuestiones sobre la seguridad de las VPN post-fusiones y adquisiciones

Las cuestiones en torno al impacto de las fusiones y adquisiciones en la infraestructura VPN existente ponen de relieve las vulnerabilidades potenciales que surgen de los cambios organizativos y la integración de redes dispares.

Un importante 69 % de los encuestados expresa su temor ante los ciberataques posteriores a las fusiones y adquisiciones, lo que evidencia la preocupación generalizada por los riesgos de seguridad asociados a estas transformaciones corporativas. Este sentimiento refleja un claro entendimiento de que las actividades de fusión y adquisición pueden desestabilizar los marcos de seguridad existentes, aumentando la exposición a las ciberamenazas.



¿Le preocupa ser víctima de un ataque tras la fusión y adquisición con su infraestructura actual?



Los períodos de transición durante las fusiones y adquisiciones presentan oportunidades únicas para que las organizaciones eliminen progresivamente las anticuadas y vulnerables tecnologías VPN en favor de marcos Zero Trust. Concretamente, las arquitecturas Zero Trust mejoran la seguridad proporcionando una segmentación completa del entorno entre usuarios y aplicaciones, cargas de trabajo y cargas de trabajo, ubicaciones de sucursales y dispositivos, ya sean dispositivos gestionados, dispositivos no gestionados, IoT o sistemas OT. Este enfoque refuerza significativamente la seguridad durante y después de una transición mediante una verificación rigurosa de todos los usuarios y dispositivos, una segmentación exhaustiva y una aplicación estricta de los controles de acceso con privilegios mínimos.

Adopción empresarial de Zero Trust

Progreso en la adopción de Zero Trust

La encuesta refleja una fuerte tendencia hacia la adopción de marcos de seguridad Zero Trust, lo que subraya el creciente reconocimiento de su importancia en la mejora de la ciberseguridad de las organizaciones. Un importante 31 % de los encuestados ya está aplicando Zero Trust (frente al 27 % en 2023), lo que indica un creciente esfuerzo proactivo para proteger mejor los recursos de la red.

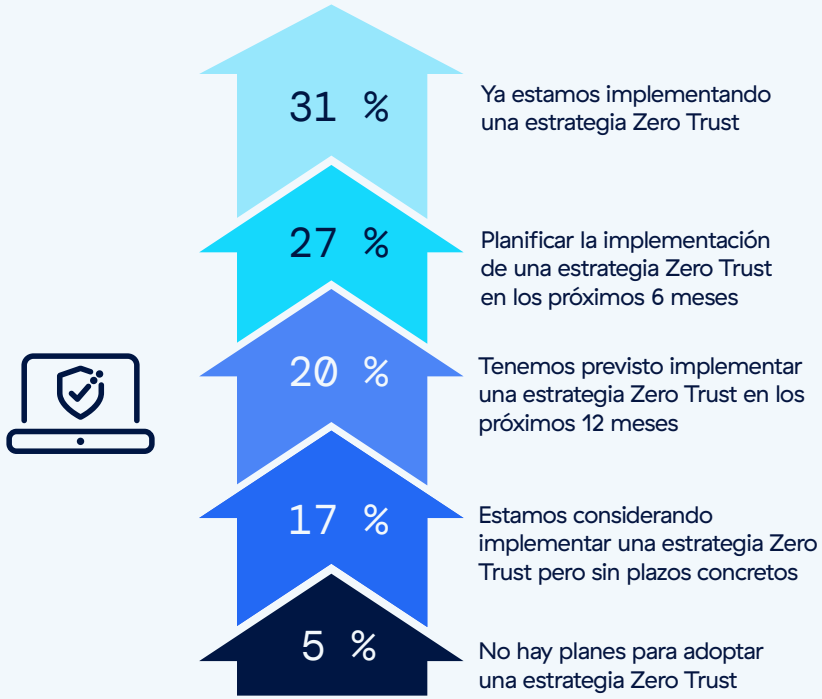
Además, el 27 % de las organizaciones tiene previsto aplicar una estrategia Zero Trust en los próximos seis meses (frente al 18 % en 2023), y otro 20 % de las organizaciones tiene previsto realizar el cambio en los próximos 12 meses, lo que demuestra un compromiso generalizado con la transición hacia Zero Trust en un futuro próximo. Esto confirma que más de tres cuartas partes de los encuestados (78 %) reconocen la urgencia y los beneficios de Zero Trust.

Sin embargo, el 17 % de los encuestados sigue considerando una estrategia Zero Trust sin un calendario concreto (frente al 23 % en 2023), lo que destaca cierta indecisión o posibles dificultades a la hora de planificar o iniciar la transición. Solo una pequeña parte (5 %) afirma no tener planes para adoptar Zero Trust (frente al 8 % en 2023), posiblemente debido a la falta de recursos.

Un análisis por tamaño de empresa indica que las organizaciones más grandes de nuestra encuesta, en particular las que tienen más de 20,000 empleados, son más propensas y rápidas a la hora de adoptar estrategias Zero Trust, con un 33 % que ya las aplica. Por el contrario, las empresas más pequeñas, de entre 1000 y 5000 empleados, muestran una tasa de adopción ligeramente inferior, del 29 %, lo que sugiere que la escala y la disponibilidad de recursos pueden influir en el ritmo y el alcance de la integración de Zero Trust.

Las organizaciones que todavía están indecisas o que planean adoptar Zero Trust deberían empezar por evaluar su postura de seguridad actual y su arquitectura de red para identificar las necesidades específicas y los desafíos potenciales.

¿Cuáles son sus planes para la adopción de una estrategia zero trust en su organización?

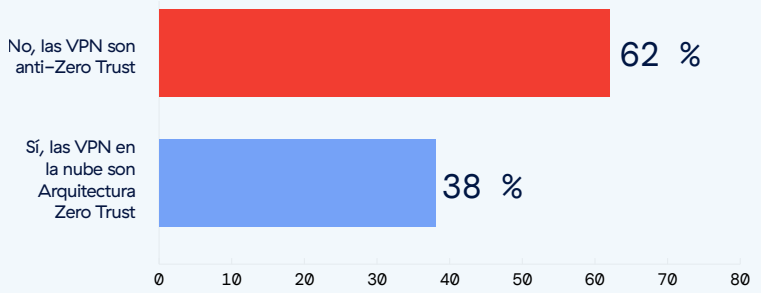


No hay seguridad Zero Trust a través de las VPN

Los resultados de la encuesta reflejan una división significativa en las creencias sobre la compatibilidad de las VPN con los marcos de seguridad Zero Trust. La mayoría (62 %) cree que las VPN son fundamentalmente “anti–Zero Trust", lo que confirma que las arquitecturas VPN tradicionales no se alinean con los principios Zero Trust. Por el contrario, el 38 % de los encuestados considera que las VPN, especialmente las plataformas basadas en la nube, son compatibles con arquitecturas Zero Trust.

Aunque esta perspectiva puede proceder de los proveedores de VPN que afirman que sus soluciones basadas en la nube se ajustan a los principios de Zero Trust, es importante analizar estas afirmaciones de manera crítica. El simple hecho de alojar un servicio VPN en la nube, por ejemplo, no confiere automáticamente atributos de Zero Trust. La seguridad Zero Trust requiere algo más que un entorno de alojamiento seguro; requiere un cambio fundamental de las defensas basadas en el perímetro a un modelo en el que la seguridad sea dinámica, granular y basada en el contexto.

¿Cree que puede lograr la seguridad Zero Trust con las VPN?



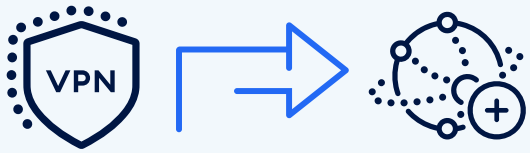
La verdadera seguridad Zero Trust pasa por la validación continua de todos los usuarios y dispositivos, la aplicación del acceso con privilegios mínimos y la segmentación del tráfico para evitar el movimiento lateral, características que las VPN tradicionales (incluso las basadas en la nube) no ofrecen. Por lo tanto, las organizaciones deben confirmar que cualquier supuesta VPN “Zero Trust" incorpora realmente estos principios básicos, en lugar de basarse únicamente en promesas de marketing.

Pasar de la VPN al acceso a la red Zero Trust

Los resultados de la encuesta muestran que la mayoría de las organizaciones están realizando un cambio estratégico, ya que el 53 % de los encuestados citaron planes para sustituir sus soluciones VPN existentes por soluciones ZTNA en un futuro próximo. El ZTNA ofrece un enfoque más flexible y seguro al aplicar políticas basadas en el contexto del usuario, la ubicación y la seguridad del dispositivo, sin asumir una confianza basada en la ubicación de la red. Esto contrasta con las VPN tradicionales, que generalmente conceden un acceso amplio a una red, lo que crea vulnerabilidades de seguridad.

Para el 53 % de las organizaciones que se encaminan hacia el ZTNA, es crucial garantizar una transición fluida planificando evaluaciones de riesgos exhaustivas, actualizando las políticas de acceso y educando a los usuarios sobre los nuevos protocolos. Mientras tanto, el 47 % que aún no tiene previsto cambiar debería evaluar sus desafíos de seguridad actuales y considerar si el ZTNA podría abordarlos de manera más eficaz que las VPN.

¿Tiene planes para sustituir su solución VPN actual por Zero Trust Network Access (ZTNA) en un futuro próximo?



53 %

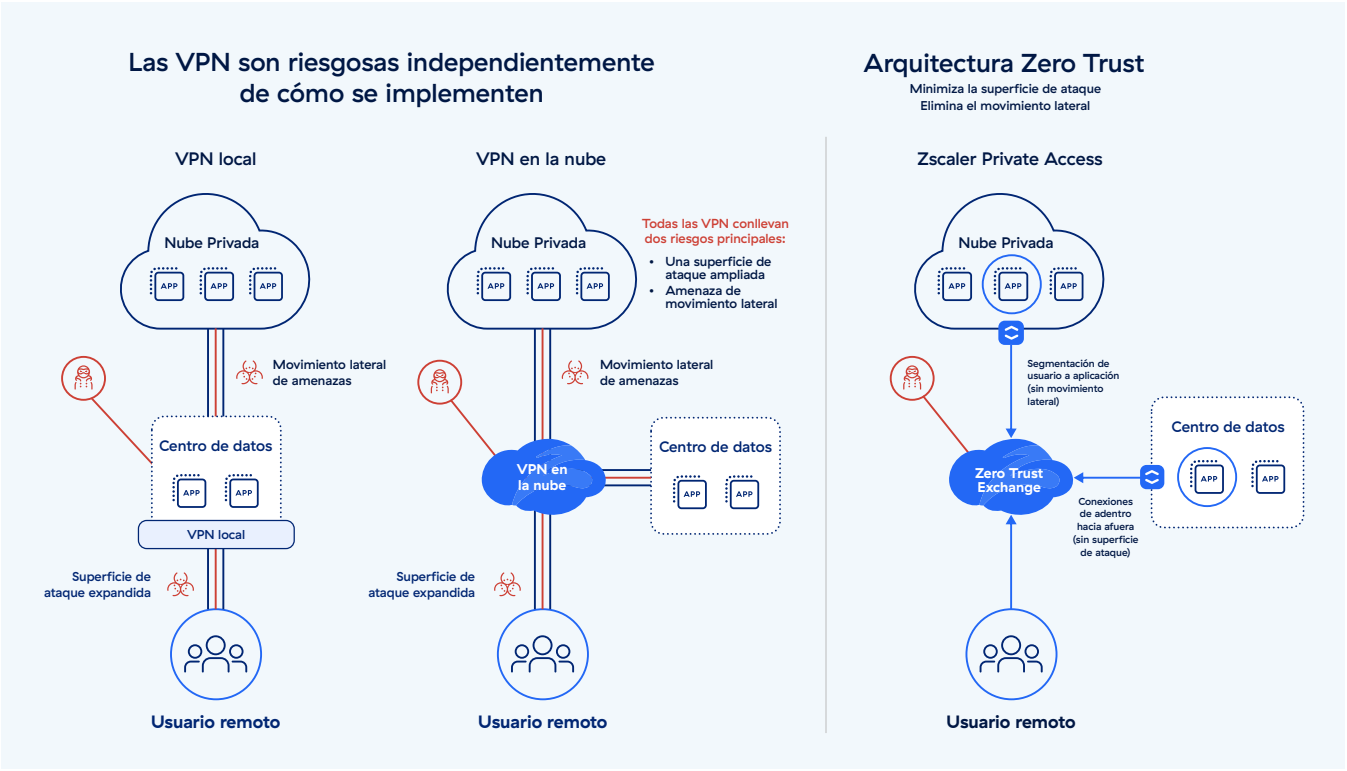
tienen planes de sustituir la VPN por una solución ZTNA en un futuro cercano

Por qué Zero Trust es más seguro que una VPN

Desde el punto de vista arquitectónico, Zero Trust y ZTNA son más seguros que las VPN tradicionales por varias razones, principalmente debido a un marco de seguridad robusto que nunca confía intrínsecamente en una única conexión. Las arquitecturas tradicionales basadas en VPN son susceptibles a un punto de falla único. Cuando una VPN o un dispositivo se ven comprometidos (por ejemplo, a través de una nueva CVE), los malintencionados pueden explotar la confianza inherente a una red plana para obtener acceso a toda la red, desplazarse lateralmente, robar datos y distribuir ransomware. Por ello, los profesionales de la seguridad están cada vez más preocupados por los riesgos de seguridad de las VPN.

Las VPN locales y en la nube presentan vulnerabilidades de seguridad similares. Además, las VPN introducen complejidad, lo que se traduce en una sobrecarga innecesaria y en tareas que consumen mucho tiempo, como el aprovisionamiento de usuarios, la gestión de tablas de enrutamiento, la solución de problemas de conectividad, la aplicación de parches, la supervisión y la optimización del rendimiento.

Con una arquitectura Zero Trust, nunca se confía en una sola conexión. Los usuarios se conectan directamente a las aplicaciones, nunca a la red subyacente. Además, cada conexión se interrumpe automáticamente, independientemente de su origen, antes de ser verificada por siete capas de controles de seguridad Zero Trust. La arquitectura Zero Trust permite a las organizaciones segmentar exhaustivamente sus entornos con un acceso granular: de usuarios a aplicaciones, de cargas de trabajo a cargas de trabajo, entre sucursales y entre dispositivos, incluidos los dispositivos IoT y OT.



Diferencias y ventajas clave

Superficie de ataque significativamente reducida
Una arquitectura Zero Trust permite una conectividad de dentro hacia fuera que oculta activos críticos, aplicaciones, servidores y mucho más de la Internet pública, al tiempo que elimina la necesidad de activos vulnerables como las VPN y los firewalls. Esto permite a las empresas ofrecer una conectividad híbrida a sus trabajadores a la vez que reducen enormemente su superficie de ataque. Por el contrario, las arquitecturas basadas en VPN y firewalls obligan a las empresas a ampliar la superficie de ataque para dar cabida a una mayor conectividad.

Verificación continua
Los modelos Zero Trust aplican una verificación de seguridad continua de las credenciales y la postura de seguridad antes de conceder el acceso a los recursos, lo que hace mucho más difícil que entidades no autorizadas obtengan y mantengan el acceso a información y sistemas confidenciales. Mientras tanto, con las VPN, el usuario o dispositivo suele tener un amplio acceso a los recursos de la red una vez que se le concede el acceso.

Acceso con privilegios mínimos
Los principios Zero Trust aplican políticas de acceso con privilegios mínimos, garantizando que los usuarios y dispositivos solo tengan acceso a los recursos necesarios para sus funciones específicas.Esto minimiza el riesgo de amenazas internas y de movimiento lateral dentro de una red, que son vulnerabilidades comunes en las configuraciones VPN.

Acceso granular y segmentación
Al dividir los recursos de red en segmentos independientes (entre usuarios y aplicaciones, entre cargas de trabajo y entre dispositivos), Zero Trust aísla las posibles violaciones en zonas más pequeñas, lo que reduce en gran medida el impacto de un ataque. Aunque las organizaciones intentan a menudo segmentar sus entornos de red, se trata de un proceso operativamente complejo y costoso que, en la práctica, suele ser incompleto, requiere cientos de reglas de firewalls discretas y expone zonas de red más amplias a los usuarios autenticados.

Potenciación de la fuerza de trabajo híbrida de la actualidad Zero Trust permite ampliar fácilmente el acceso ultrarrápido a las aplicaciones privadas a los usuarios remotos, además de a la sede central, las sucursales y los socios externos.

Mejora de la experiencia del usuario y reducción de la complejidad
Zero Trust mejora las experiencias de los usuarios al eliminar la necesidad de que todo el tráfico remoto pase por un punto de red central, un cuello de botella de rendimiento habitual con las VPN. Esta arquitectura puede gestionar mejor los requisitos de escalabilidad de las redes modernas que incluyen IoT y políticas BYOD. Además, Zero Trust reduce la sobrecarga de gestión al automatizar los controles de seguridad y simplificar la aplicación de las políticas de seguridad en toda la red.

Estas ventajas arquitectónicas hacen de Zero Trust una alternativa convincente a las VPN tradicionales, particularmente en el panorama de amenazas cada vez más sofisticado y distribuido de la actualidad. Para las organizaciones que buscan reforzar sus defensas de ciberseguridad, la adopción de un enfoque Zero Trust proporciona una infraestructura de seguridad más sólida, flexible y escalable.

Predicciones sobre VPN para 2024 y el futuro

1 Aumentarán las vulnerabilidades y los exploits graves de las VPN

Dada la frecuencia, gravedad y escala de las vulnerabilidades de las VPN reveladas el año pasado, las empresas pueden esperar que esta tendencia continúe. Los malintencionados y los investigadores de seguridad son conscientes del elevado riesgo de vulnerabilidades de alta gravedad en los productos de VPN. A su vez, están buscando activamente algo más, por lo que es probable que se encuentren más CVE en los próximos meses y años.

2 Los ataques de alto perfil causados por las VPN serán el centro de atención

En estrecha relación con nuestra primera predicción, veremos más grandes organizaciones revelar violaciones de seguridad derivadas de vulnerabilidades de VPN explotadas. En parte, esto se deberá a las nuevas directrices de regulación de la SEC, que exigen a las empresas que cotizan en bolsa que divulguen información detallada sobre las violaciones que tengan un impacto material. Como ya hemos visto, los malintencionados crean sistemáticamente puertas traseras en los entornos de destino cuando se producen vulnerabilidades de VPN, con el fin de explotarlas en el futuro, incluso después de que estas vulnerabilidades hayan sido parcheadas. A medida que transcurra el año, empezarán a divulgarse más en los archivos públicos de la SEC y llegarán a las noticias.

3 Un aumento en las ofertas de VPN impulsadas por la IA generará cuestiones sobre la seguridad y la privacidad

En medio de los continuos avances en IA, las soluciones VPN potenciadas por IA inundarán el mercado. Sin embargo, las empresas deberían evaluar estas ofertas cautelosamente. Aunque prometan un mayor rendimiento, la integración de la IA amplificará los riesgos de seguridad y aumentará las oportunidades de que los atacantes exploten las vulnerabilidades de las VPN. Además, surgirán problemas de privacidad debido al amplio análisis de datos que aumenta el riesgo de que se exponga información confidencial.

4 Los ataques de repetición de contraseñas a las VPN seguirán creciendo

Los atacantes encontrarán cada vez más maneras de aprovecharse de las malas prácticas de gestión de contraseñas y de los perfiles de conexión VPN por defecto no utilizados a través de ataques de repetición de contraseñas. En estos ataques, los malintencionados prueban la misma contraseña en muchas cuentas VPN hasta que logran entrar, obteniendo un acceso no autorizado. Dado que muchas de las recientes violaciones de VPN de alto perfil han aprovechado eficazmente esta técnica, las empresas deberán prever ataques similares.

5 El gasto empresarial se desviará de las VPN hacia la conectividad Zero Trust

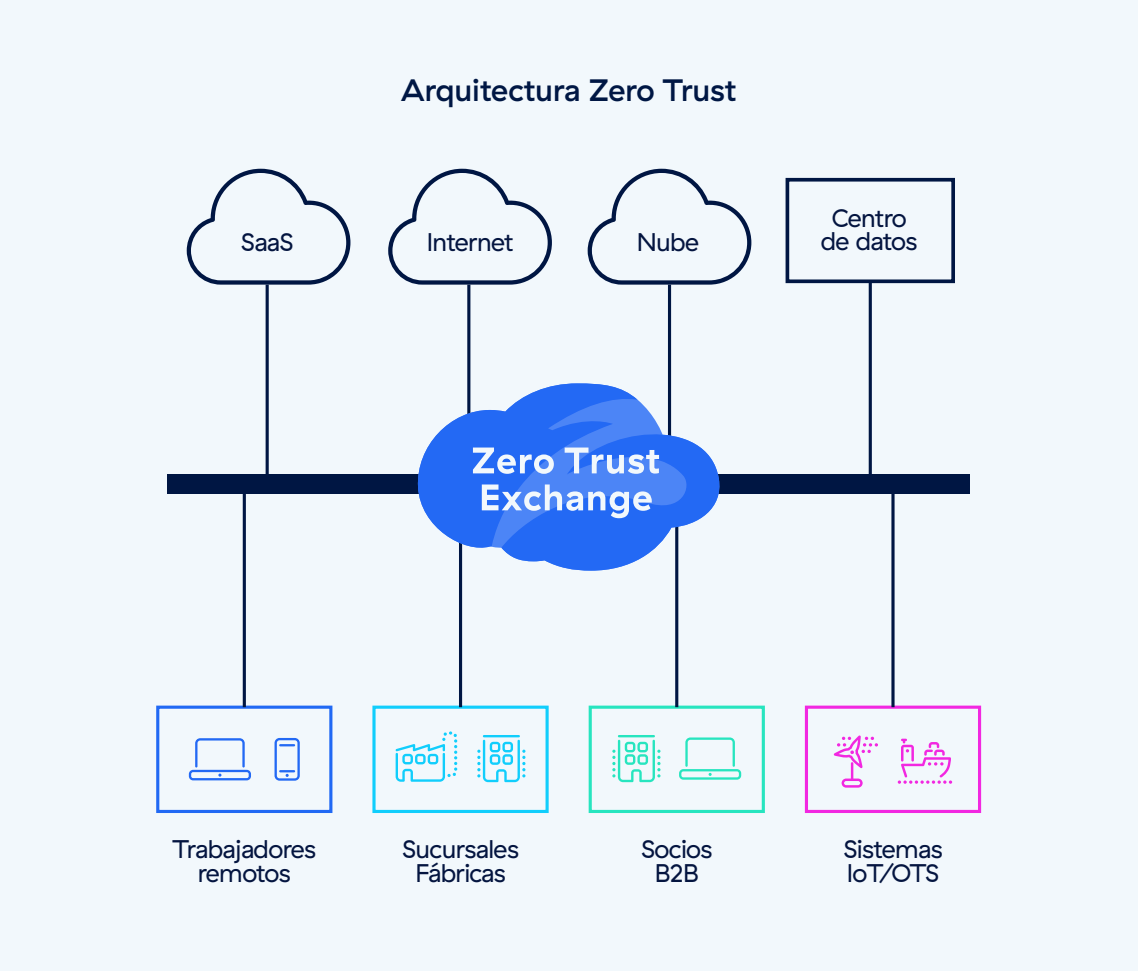
Aunque las VPN llevan mucho tiempo permitiendo la conectividad remota de las empresas, los constantes y crecientes problemas de seguridad de esta tecnología harán que sea más difícil justificar el gasto a largo plazo. A medida que las empresas logren un consenso en torno a Zero Trust como arquitectura preferida para la seguridad y la conectividad, los presupuestos empresariales seguirán orientándose hacia iniciativas Zero Trust para proteger a los trabajadores remotos.

Cómo Zscaler permite el reemplazo de VPN y la transformación Zero Trust

Los firewalls tradicionales y las VPN crean una superficie de ataque masiva que permite a los atacantes ver y explotar los recursos expuestos. Al colocar a los usuarios en la red y permitirles acceder a cualquier aplicación alojada en ella, estos enfoques heredados facilitan a los atacantes el acceso a datos confidenciales. Hacen que sea difícil y lleve mucho tiempo proporcionar acceso o compartir recursos de manera segura con terceros proveedores, contratistas y agencias. Además, aumentan los costos y la complejidad, y son demasiado lentos para dar servicio a la fuerza de trabajo híbrida actual.

La plataforma Zscaler Zero Trust Exchange™, la mayor nube de seguridad en línea del mundo, conecta de manera segura usuarios, cargas de trabajo, IoT/OT y socios B2B sin ampliar el acceso a la red.

Zscaler Private Access™ (ZPA™), una parte esencial de Zero Trust Exchange, proporciona acceso directo a las aplicaciones privadas ocultas detrás de Zero Trust Exchange, minimizando la superficie de ataque, permitiendo una segmentación granular 1:1 de usuario a aplicación, eliminando el movimiento lateral y ofreciendo protección de aplicaciones privadas e inspección de tráfico en línea mientras detiene las amenazas de día cero, potenciando su postura de seguridad. Como servicio nativo en la nube, ZPA puede implementarse en cuestión de horas para sustituir a las herramientas de acceso remoto heredadas, como las VPN y las VDI.



Zero Trust Networking

ZPA permite un acceso granular y segmentado con conectividad de adentro hacia afuera a aplicaciones y cargas de trabajo privadas. Además, ZPA incluye una amplia gama de servicios de control de acceso, entre los que se incluyen la segmentación de usuario a aplicación impulsada por la IA con recomendaciones automatizadas para las políticas de acceso de los usuarios y los segmentos de aplicaciones, la segmentación de carga de trabajo a carga de trabajo, el acceso remoto privilegiado, el perímetro de servicio privado, el acceso al navegador y mucho más.

Protección contra ciberamenazas

ZPA ofrece capacidades avanzadas de ciberprotección para proteger su organización. Entre ellas se incluyen las capacidades de protección de aplicaciones que utilizan la inspección de seguridad en línea para detener los ataques a aplicaciones más frecuentes y las vulnerabilidades de día cero, así como la tecnología de engaño que atrae a los atacantes con aplicaciones señuelo y facilita la detección de amenazas sofisticadas.

Protección de datos

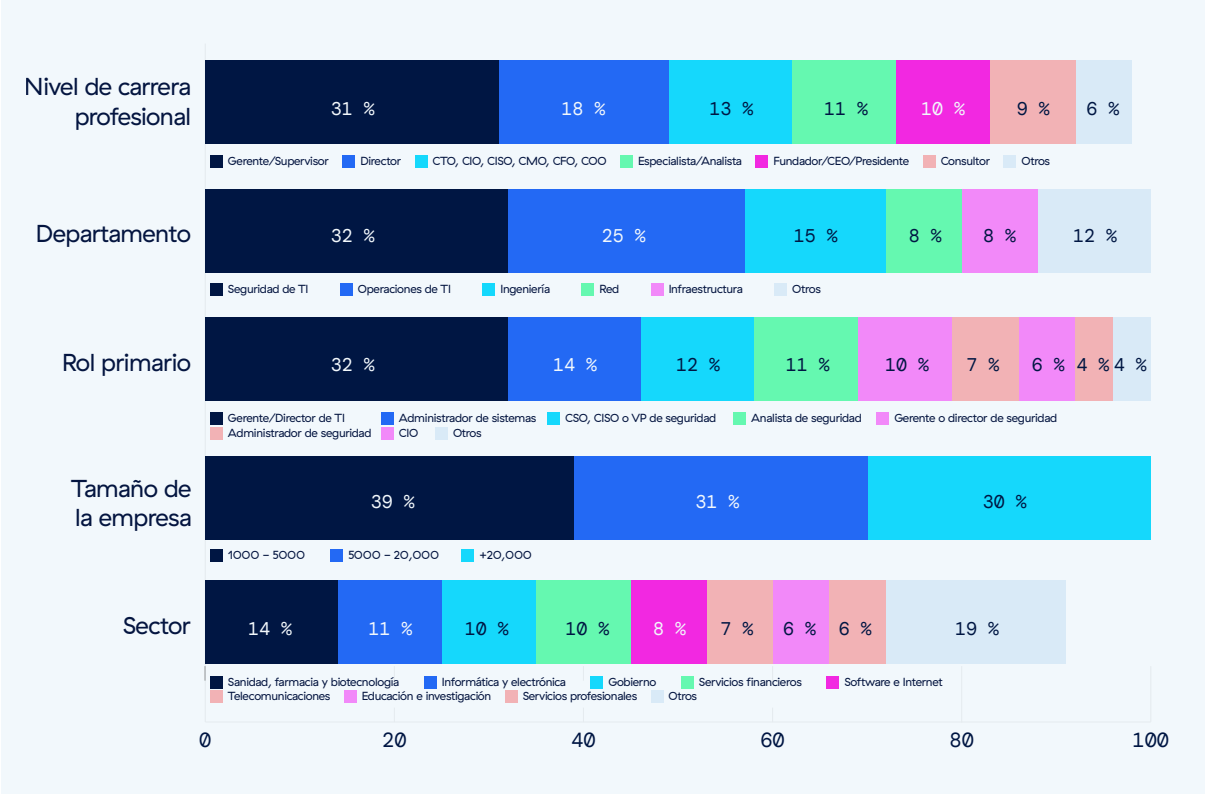
ZPA proporciona una protección de datos integral y detiene la pérdida de datos en todos los canales con Prevención de Pérdida de Datos (DLP) web, DLP de punto final y aislamiento del navegador que evita la fuga de datos para usuarios vulnerables y puntos finales en dispositivos BYOD.

Mejores prácticas para contrarrestar los riesgos de las VPN

- **Minimizar la superficie de ataque:** Proporcione acceso directo a las aplicaciones, garantizando que tanto las aplicaciones como los usuarios sean invisibles a Internet, impidiendo eficazmente que los atacantes las descubran y exploten para obtener un acceso inicial.
- **Prevenga el compromiso inicial:** Inspeccione todo el tráfico en línea para detener automáticamente los exploits de día cero, el malware y otras amenazas sofisticadas.
- **Bloquee el acceso no autorizado:** Utilice una autenticación multifactor fuerte (MFA) como contraseñas de un solo uso o tokens, biometría o credenciales FIDO2 para validar las solicitudes de acceso de los usuarios. Por el contrario, la MFA débil suele recurrir a enfoques que emplean preguntas de restablecimiento de contraseña.
- **Imponga el acceso con privilegios mínimos:** Restrinja los permisos para usuarios, tráfico, sistemas y aplicaciones en función de la identidad y el contexto, garantizando que solo los usuarios autorizados puedan acceder a los recursos aprobados (proporcionando seguridad adicional en casos de compromiso de la MFA o robo de credenciales).
- **Elimine el movimiento lateral:** Conecte a los usuarios directamente a las aplicaciones, no a la red, para limitar el radio de alcance de un posible incidente y mitigar el riesgo de movimiento lateral de las amenazas.
- **Bloquee a los usuarios comprometidos y las amenazas internas:** Habilite la inspección y supervisión en línea para detectar usuarios comprometidos con acceso a su red, aplicaciones privadas y datos.
- **Detenga la pérdida de datos:** Inspeccione los datos en movimiento y los datos en reposo para detener el robo activo de datos durante un ataque.
- **Implemente defensas activas:** Aproveche la tecnología de engaño con señuelos y realice una inspección diaria de amenazas para frustrar y capturar los ataques en tiempo real.
- **Ponga a prueba su postura de seguridad:** Obtenga evaluaciones periódicas de riesgos por parte de terceros y lleve a cabo actividades de equipo puramente para identificar y endurecer las brechas de su programa de seguridad. Solicite a sus proveedores de servicios y socios tecnológicos que hagan lo mismo y comparta los resultados de estos informes con su equipo de seguridad.

Metodología y Demografía

Este informe se basa en los resultados de una exhaustiva encuesta en línea a 647 profesionales de la informática y la ciberseguridad, realizada en abril de 2024 para identificar las últimas tendencias de adopción, los problemas, las carencias y las preferencias de soluciones relacionadas con el riesgo de las VPN por parte de las empresas. Los encuestados van desde ejecutivos técnicos hasta profesionales de seguridad de TI, que representan una sección transversal equilibrada de organizaciones de diferentes tamaños en varios sectores.



Acerca de Zscaler

Zscaler 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 más información, visite www.zscaler.com.mx.

Acerca de ThreatLabZ

ThreatLabz es la división de investigación de seguridad de Zscaler. Este equipo de clase mundial es responsable de localizar nuevas amenazas y asegurar que las miles de organizaciones que utilizan la plataforma global de Zscaler estén siempre protegidas. Además de investigar el malware y analizar el comportamiento, los miembros del equipo participan en la investigación y el desarrollo de nuevos módulos prototipo para la protección contra amenazas avanzadas en la plataforma Zscaler y realizan regularmente auditorías de seguridad internas para garantizar que los productos y la infraestructura de Zscaler cumplan con los estándares de cumplimiento de la seguridad. ThreatLabz publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal, research.zscaler.com.

Acerca de Cybersecurity Insiders

Cybersecurity Insiders reúne a más de 600,000 profesionales de la seguridad informática y a proveedores de tecnología de talla mundial para facilitar la resolución inteligente de problemas y la colaboración a la hora de resolver los problemas de ciberseguridad más críticos de la actualidad.

Nuestro enfoque se centra en crear y dirigir contenidos únicos que eduquen e informen a los profesionales de la ciberseguridad sobre las últimas tendencias, soluciones y mejores prácticas en este ámbito. Desde exhaustivos estudios de investigación y revisiones imparciales de productos hasta prácticas guías electrónicas, interesantes seminarios web y artículos educativos, nos comprometemos a proporcionar recursos que ofrezcan respuestas basadas en evidencia a los complicados problemas que plantea la ciberseguridad actualmente.

Póngase en contacto con nosotros hoy mismo para saber cómo Cybersecurity Insiders puede ayudarle a distinguirse en un mercado saturado e impulsar la demanda, la visibilidad de marca y la presencia de liderazgo intelectual.

Envíenos un email a info@cybersecurity-insiders.com o vaya a cybersecurity-insiders.com.

Experimente su mundo, protegido.

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**.

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134