Informe de riesgo de VPN de 2023

Cybersecurity INSIDERS

Resumen

Tradicionalmente, las redes privadas virtuales (VPN) han facilitado el acceso remoto básico. El rápido crecimiento del personal distribuido y la creciente adopción de las tecnologías en la nube están poniendo en jaque la conectividad básica que ofrece VPN. A medida que el panorama de amenazas evoluciona rápidamente, las VPN no pueden proporcionar el acceso seguro y segmentado que necesitan las organizaciones. Por el contrario, las VPN a menudo brindan acceso completo a la red corporativa, lo que aumenta las posibilidades de ataques cibernéticos una vez que los delincuentes obtienen acceso a través de las credenciales de inicio de sesión. Además, las VPN conectan múltiples sitios, permiten el acceso a terceros, admiten dispositivos no administrados y permiten la conectividad de dispositivos IoT. Sin embargo, estos diversos casos de uso llevan las VPN más allá de su propósito y diseño iniciales, lo que a menudo crea brechas de seguridad ante un panorama de amenazas cada vez más complejo y cambiante.

Este completo informe, basado en una encuesta a 382 profesionales de TI y expertos en ciberseguridad, explora las diferentes facetas de estos desafíos de seguridad y experiencia del usuario. El Informe de riesgo de VPN de 2023 revela la complejidad de la gestión de VPN actual, los problemas de experiencia del usuario, las vulnerabilidades a diversos ataques cibernéticos y su potencial para afectar la postura de seguridad más amplia de las organizaciones. El informe también describe modelos de seguridad más potentes, en los que la confianza cero surge como una opción viable para asegurar y acelerar la transformación digital.

LOS HALLAZGOS CLAVE DE LA ENCUESTA INCLUYEN:

Vulnerabilidades de VPN e impactos en la seguridad cibernética: A pesar de su papel fundamental, las VPN presentan riesgos de seguridad, y el 88 % de las organizaciones expresan una preocupación entre leve a extrema de que las VPN puedan poner en peligro la seguridad de su entorno. Además, el 45 % de las organizaciones confirmaron haber experimentado al menos un ataque que aprovechó las vulnerabilidades de VPN en los últimos 12 meses: una de cada tres fue víctima de ataques de ransomware relacionados con VPN. La creciente amenaza de los ciberatacantes que explotan las vulnerabilidades de las VPN subraya la necesidad urgente de abordar la seguridad de las arquitecturas VPN actuales.

Uso de VPN y experiencia del usuario: las VPN tienen un amplio espectro de uso, y el 84 % de los encuestados identifica el acceso remoto de los empleados como su aplicación principal. Sin embargo, los usuarios informaron de una experiencia menos que óptima, con una mayoría de usuarios insatisfechos con su experiencia VPN (72 %), lo que pone de manifiesto la necesidad de soluciones de acceso remoto más fáciles de usar y confiables en el lugar de trabajo digital.

Continuación del resumen

Principales vectores de ataque: una de cada dos organizaciones se ha enfrentado a ataques relacionados con VPN en el último año. Los vectores de ataque de VPN necesitan una atención especial debido a sus funciones críticas en las operaciones comerciales y la comunicación. Además, los usuarios de terceros, como contratistas y proveedores, sirven como puertas traseras potenciales para el acceso malicioso a las redes, lo que complica aún más el trabajo de los equipos de seguridad de la red. En la encuesta, 9 de cada 10 encuestados expresaron su preocupación por los terceros que actúan como posibles puertas traseras en sus redes a través del acceso VPN.

Aceptar la confianza cero: la transición a un modelo de confianza cero es una prioridad en la agenda de la mayoría de las organizaciones. Alrededor de 9 de cada 10 encuestados identificaron la adopción de la confianza cero como un objetivo importante, y más de una cuarta parte (el 27 %) ya están implementando la confianza cero. El 37 % de los encuestados tiene previsto reemplazar su VPN con soluciones Zero Trust Network Access (ZTNA).

Estamos agradecidos a Zscaler por su contribución a esta encuesta de riesgo de VPN. Su experiencia en soluciones de confianza cero y acceso seguro ha enriquecido significativamente nuestros resultados.

Estamos seguros de que las conclusiones de este informe serán un recurso esencial para los profesionales de TI y ciberseguridad en su viaje hacia la seguridad de confianza cero.

Gracias,

Holger Schulze

Holger Schulze
Director general y fundador
Cybersecurity Insiders

Cybersecurity
INSIDERS

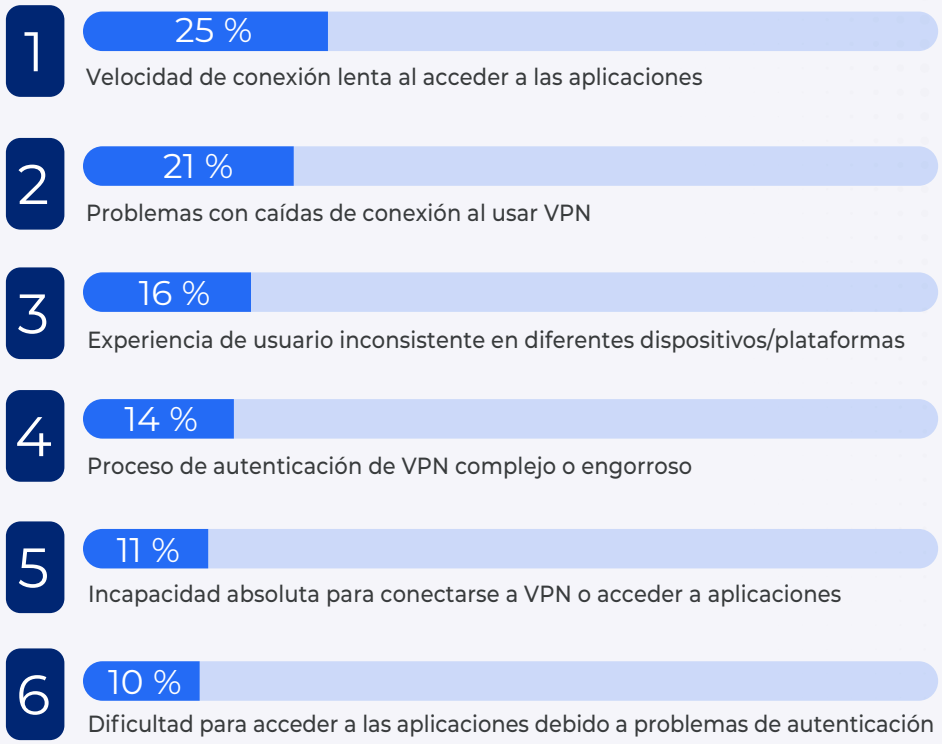
Los usuarios finales luchan con la VPN

Entre los problemas de VPN encontrados, la velocidad de conexión lenta al acceder a aplicaciones a través de VPN es el más frecuente, señalado por el 25 % de los encuestados. Otras contrariedades importantes incluyen problemas con caídas de conexión al usar VPN (el 21 %) y una experiencia de usuario inconsistente en diferentes dispositivos/plataformas (el 16 %).

Dados estos hallazgos, es evidente que mejorar la experiencia del usuario en su acceso remoto debería ser una prioridad para muchas organizaciones. Una experiencia de acceso fluida y confiable no sólo contribuye a la productividad, sino que también puede mejorar la seguridad al fomentar el cumplimiento de las políticas de seguridad.

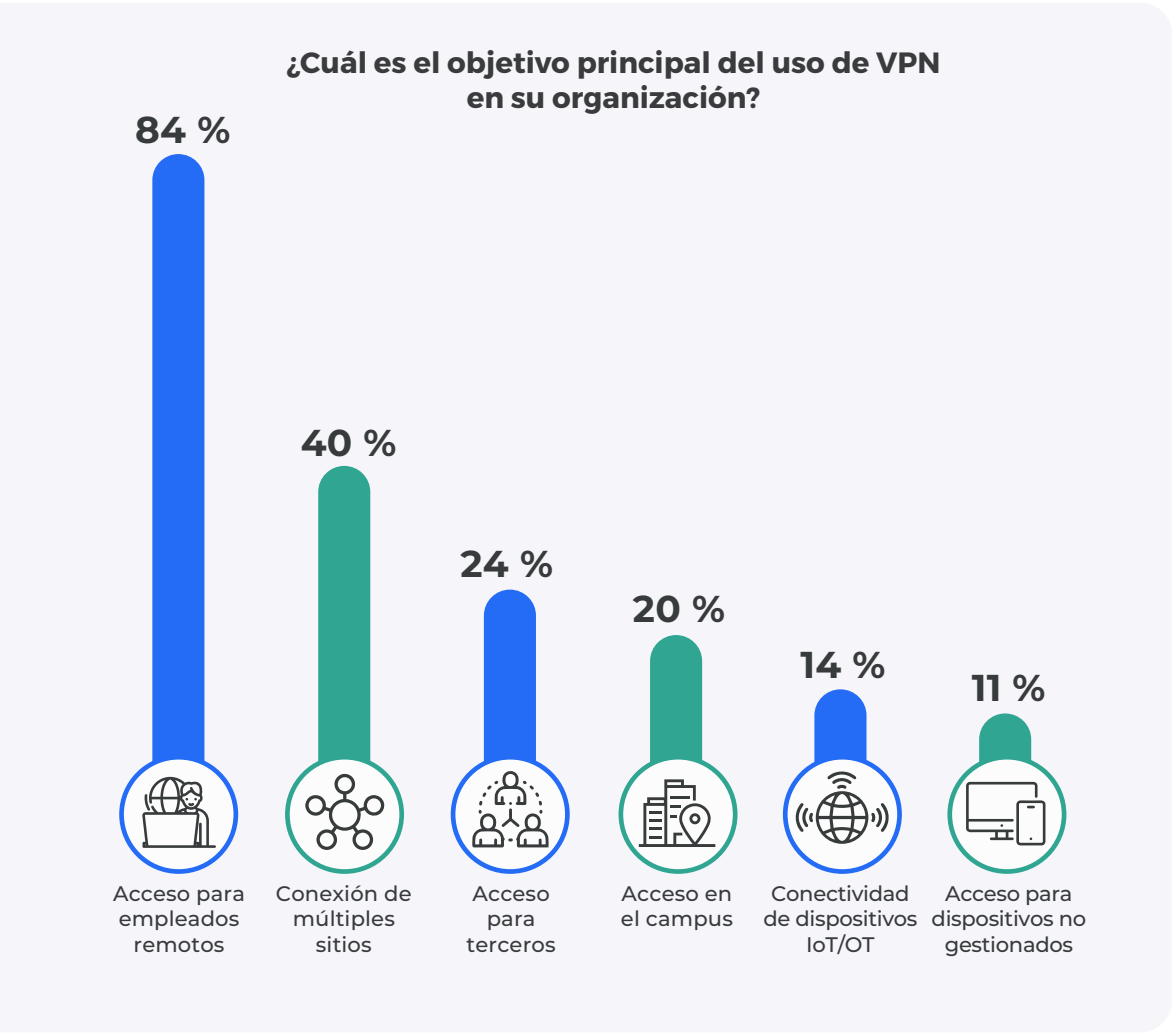
Las mejoras pueden variar desde optimizar el rendimiento de la red hasta minimizar las velocidades de conexión lentas y las caídas de conexión, simplificar el proceso de autenticación de VPN y garantizar una experiencia de usuario uniforme en diferentes plataformas. También es fundamental contar con mecanismos de soporte sólidos para ayudar a los usuarios a solucionar problemas y resolver cualquier dificultad que puedan encontrar al usar la VPN.

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



Otro 3 %

Caso de uso principal de VPN: acceso remoto para empleados



Otro 3 %

Las VPN llevan empleándose mucho tiempo para conectar empleados remotos a la red de la organización y facilitar una variedad de casos de uso, como el trabajo remoto y las conexiones de terceros.

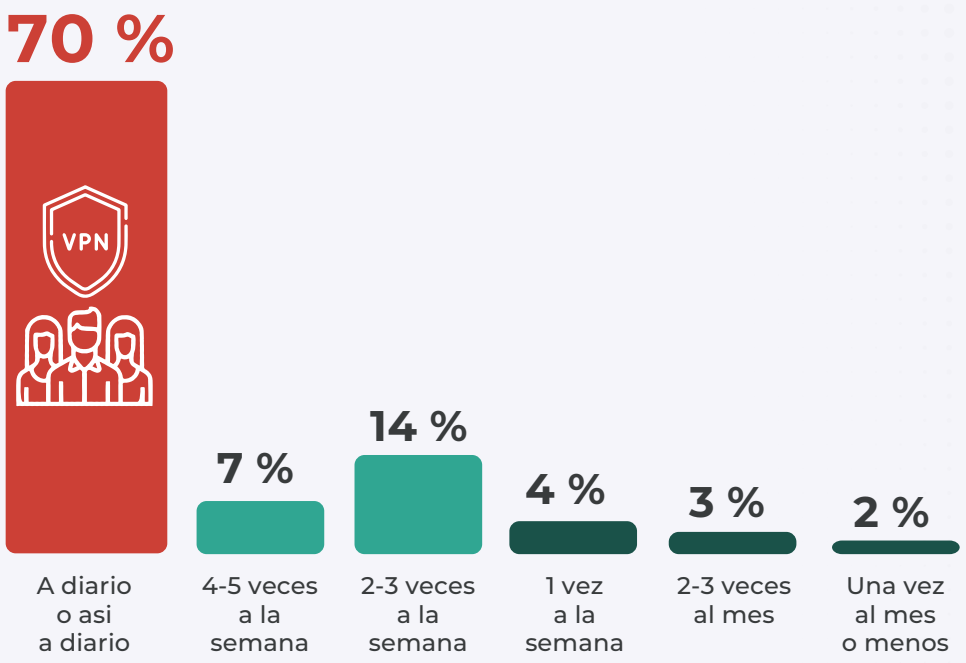
El objetivo principal de las VPN en la mayoría de las organizaciones (el 84 %) es permitir el acceso de los empleados remotos. Esto es un reflejo de la tendencia del trabajo remoto, que ha aumentado significativamente en los últimos años. Sin embargo, es interesante que sólo el 11 % utilice VPN para administrar el acceso de dispositivos no administrados, lo que apunta a un área de vulnerabilidad a la que es posible que las organizaciones no estén atendiendo como es debido.

Alta dependencia de VPN

Una cantidad significativa de usuarios finales (el 70 %) utiliza VPN a diario o casi a diario, lo que demuestra una alta dependencia de las VPN para las operaciones comerciales diarias y rutinarias. Sumados a los que usan VPN 4 o 5 veces por semana, el 77 % de todos los encuestados utiliza la VPN para su trabajo casi todos los días. Curiosamente, ninguno de los encuestados indicó que usa la VPN menos de una vez al mes, lo que confirma la adopción generalizada de la tecnología.

Dada esta alta frecuencia de uso, es vital garantizar la disponibilidad constante y la seguridad potente de los servicios de acceso remoto/VPN.

¿Con qué frecuencia utilizan sus usuarios finales la VPN?



Problemas de experiencia del usuario

¿Cuál es el problema más importante al que se enfrenta su organización con su servicio VPN actual?

32 %
Mala experiencia de usuario (conexiones lentas, desconexiones frecuentes, etc.)

14 %
Costes elevados (infraestructura, licencias, mantenimiento, etc.)

13 %
Dificultad para integrarse con otros sistemas y servicios

12 %
Gestión y administración complejas

Limitaciones de escalabilidad y flexibilidad 11 % | Seguridad y cumplimiento insuficientes 7 % | Soporte inadecuado para el trabajo remoto y la colaboración 4 % | Otros 7 %

El rendimiento y la experiencia del usuario de los servicios VPN afectan significativamente a la productividad y la eficiencia operativa general de las organizaciones. Una VPN que es lenta o se desconecta con frecuencia puede interrumpir significativamente las operaciones comerciales y frustrar a los usuarios. En cuanto a los resultados de la encuesta, el problema más importante detectado en relación a los servicios de VPN es la mala experiencia del usuario: un 32 % de los encuestados cita conexiones lentas y desconexiones frecuentes.

Dados estos resultados, las organizaciones deberían priorizar la mejora de la experiencia del usuario de sus servicios de acceso remoto, lo que podría implicar aumentar la capacidad del servidor o elegir soluciones de acceso seguro conocidas por su velocidad y estabilidad. Curiosamente, las organizaciones clasificaron la seguridad como un problema relativamente poco importante a pesar de los varios ataques cibernéticos a VPN sucedidos en los últimos años.

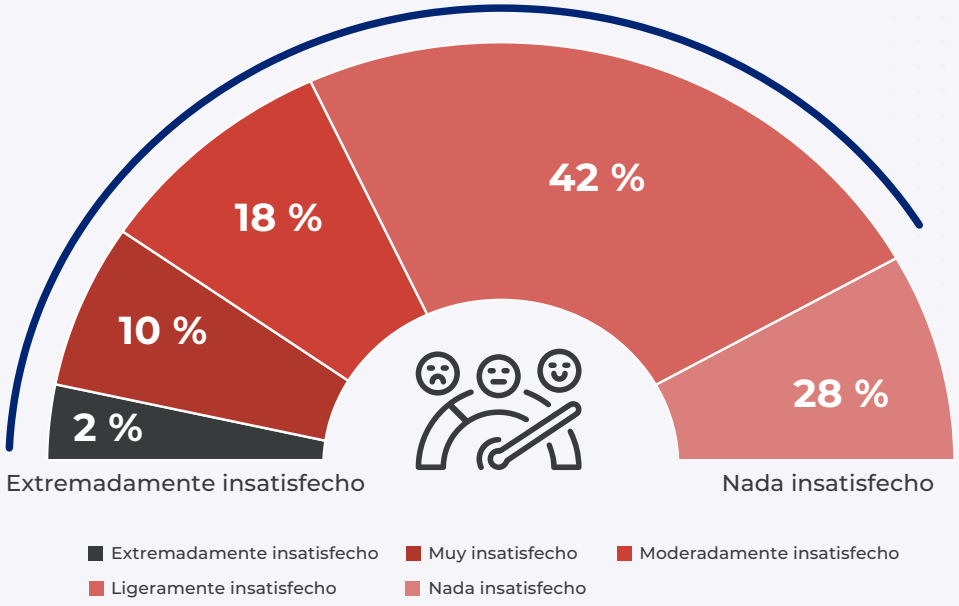
Insatisfacción del usuario con la VPN

Evaluar la satisfacción del usuario con la experiencia de VPN es fundamental, ya que la insatisfacción no sólo afecta la productividad, sino que también puede conducir al incumplimiento de las políticas de seguridad, lo que a su vez podría generar vulnerabilidades de seguridad.

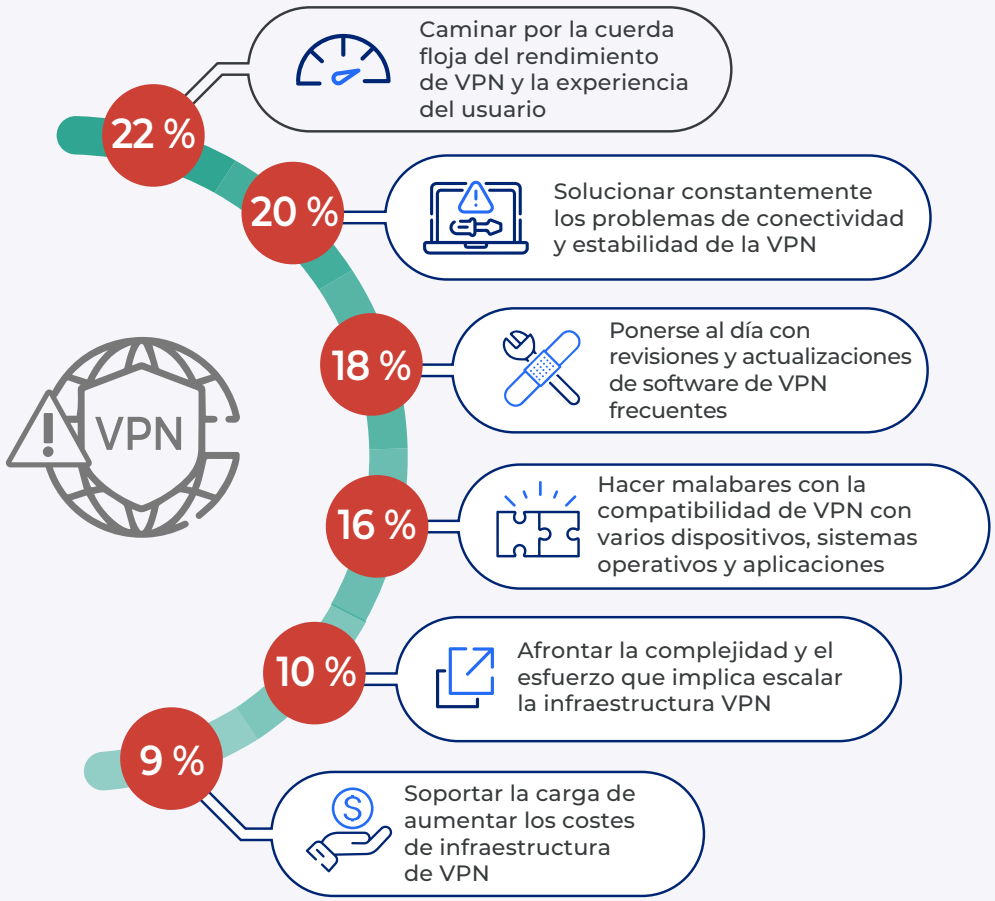
Una gran mayoría de usuarios (el 72 %) no están satisfechos con su experiencia de VPN, lo que pone de manifiesto la necesidad de soluciones de acceso remoto más fáciles de usar y confiables en el lugar de trabajo digital.

¿Hasta qué punto están sus usuarios insatisfechos con su experiencia VPN?

El **72 %** de las organizaciones están entre ligeramente y extremadamente insatisfechas con su experiencia VPN



Desafíos de la gestión de VPN



Otro 5 %

La encuesta revela que el mayor quebradero de cabeza en la gestión de la infraestructura de VPN, según indica el 22 % de los encuestados, es equilibrar el rendimiento de la VPN con la experiencia del usuario.

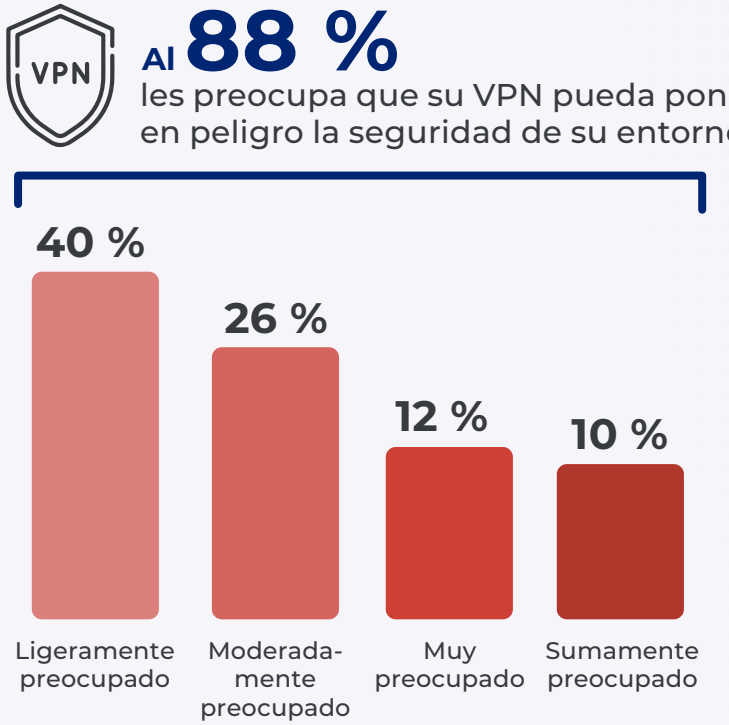
La solución de problemas de conectividad y estabilidad de la VPN también es una preocupación importante que afecta a casi el 20 % de los encuestados, seguida de cerca por el esfuerzo necesario para mantenerse al día con las revisiones y actualizaciones de software frecuentes (18 %). Curiosamente, sólo el 9 % de los encuestados mencionan el aumento de los costes de la infraestructura VPN como su mayor quebradero de cabeza.

Preocupaciones de seguridad de VPN

El nivel de seguridad que brinda una solución de acceso remoto es vital para proteger los datos y sistemas confidenciales de las organizaciones. Frente a amenazas cibernéticas cada vez más avanzadas, las VPN pueden fortalecer o comprometer la postura de seguridad de una organización, según su diseño y cómo se administren.

Al revisar los resultados de la encuesta, a la gran mayoría de los encuestados (el 88 %) les preocupa que su VPN pueda poner en peligro la seguridad de su entorno. Particularmente digno de mención es que un 22 % combinado de los encuestados informan estar "muy" o "sumamente" preocupados, lo que indica un nivel significativo de ansiedad en torno a las VPN como posibles puntos débiles de seguridad.

¿Hasta qué punto le preocupa que la VPN pueda poner en peligro su capacidad de mantener la seguridad de su entorno?

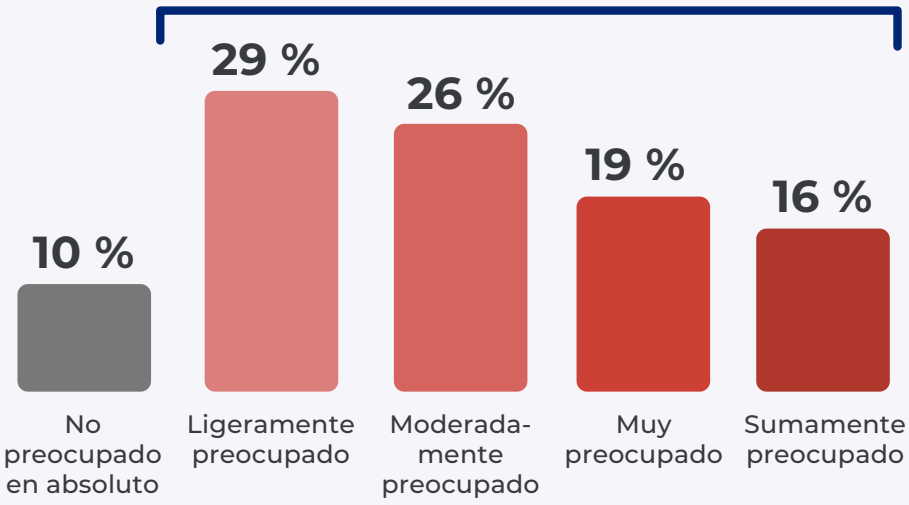


Preocupaciones de seguridad de terceros

¿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?

Al **90 %**

le preocupan los terceros que actúan como puertas traseras potenciales en sus redes a través del acceso VPN



Otorgar acceso a terceros a través de una VPN es una práctica comercial necesaria, pero también plantea serios problemas de seguridad. Dado que las entidades de terceros pueden no adherirse a los mismos estándares estrictos de ciberseguridad, potencialmente pueden proporcionar una puerta trasera para que los atacantes cibernéticos vulneren la red de una organización.

En la encuesta, una gran mayoría de los encuestados (el 90 %) expresó su preocupación por los terceros que actúan como posibles puertas traseras en sus redes a través del acceso VPN. Un total combinado del 35 % indicaron estar "muy" o "sumamente" preocupados, lo que sugiere que el acceso a VPN de terceros es una fuente importante de ansiedad.

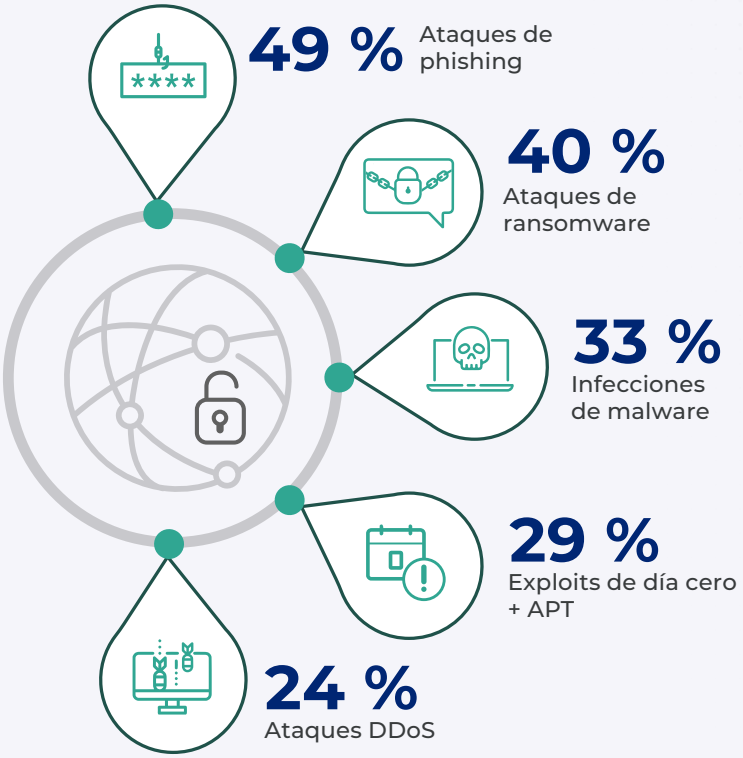
Las organizaciones deberían aplicar medidas de seguridad rigurosas al otorgar acceso VPN a terceros. Hacerlo podría implicar la revisión y actualización periódica de los permisos de acceso, la aplicación de políticas de contraseñas seguras y el control de la actividad de la red en busca de anomalías. Además, las organizaciones deben asegurarse de que los terceros cumplan con sus políticas de seguridad cibernética y considerar el uso de tecnologías avanzadas como las arquitecturas de confianza cero, que sólo otorgan acceso cuando es necesario.

Los ataques de phishing representan la mitad de los ciberataques

Las VPN tienen un largo historial de vulnerabilidades y requieren que los equipos de TI revisen constantemente sus servidores VPN. Esto puede exponer potencialmente a una organización a una variedad de ataques cibernéticos a medida que los autores de amenazas continúan volviéndose más sofisticados y creativos en sus técnicas.

Los encuestados ven los ataques de phishing (el 49 %) y los ataques de ransomware (el 40 %) como los tipos de ataques más probables para explotar las vulnerabilidades de VPN de su organización. Estos ataques a menudo implican engañar a los usuarios para que revelen información confidencial o implementen software malicioso que bloquea los sistemas hasta que se paga un rescate.

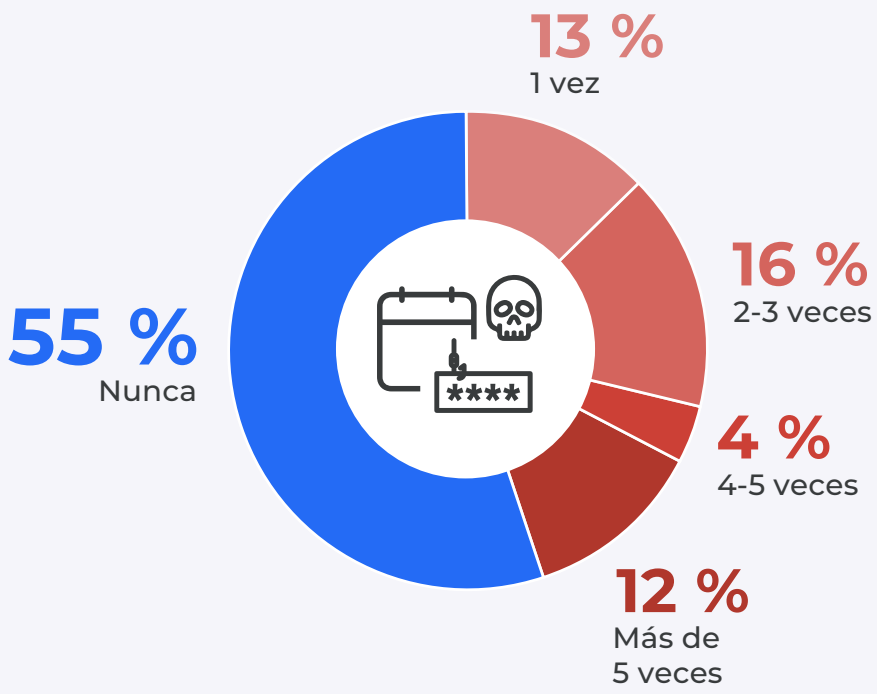
¿Qué tipos de ciberataques cree que es más probable que aprovechen las vulnerabilidades de VPN de su organización?



Ataques de intermediarios 22 % | Ataques de escalada de privilegios 20 % | Ataques de exfiltración de datos 18 % | Ataques de fuerza bruta 11 % | Secuencias de comandos entre sitios 11 % | Ejecución remota de código 9 %

1 de cada 2 organizaciones ha experimentado ataques relacionados con VPN

En los últimos 12 meses, ¿su organización ha experimentado algún ataque que haya aprovechado las vulnerabilidades de seguridad en sus servidores VPN?



La seguridad de un servidor VPN es crucial para mantener la integridad y confidencialidad de los datos que maneja. Como las organizaciones dependen cada vez más de las VPN para el trabajo remoto, cualquier vulnerabilidad puede convertirse en un objetivo atractivo para los ciberatacantes.

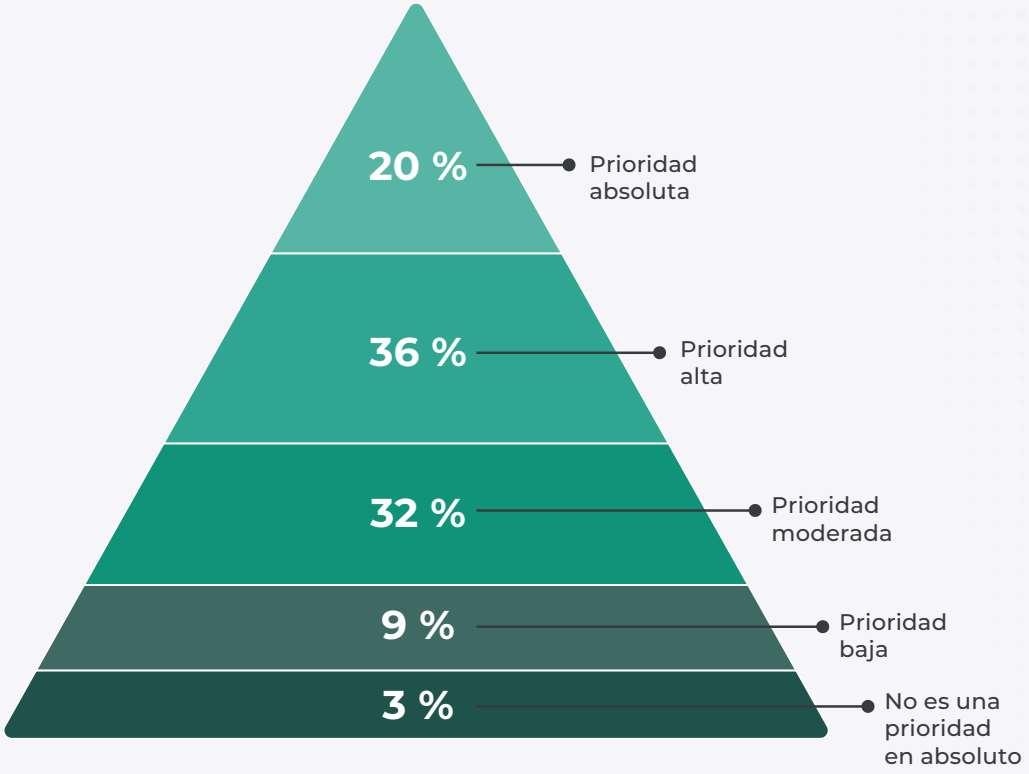
Según la encuesta, una parte considerable de las organizaciones (el 45 %) experimentó uno o más ataques en sus servidores VPN en los últimos 12 meses. Dichos ataques aprovecharon las vulnerabilidades del software en los servidores VPN, lo que pone de relieve la necesidad urgente de soluciones de acceso remoto más seguras.

La estrategia de confianza cero es una gran prioridad

La adopción de la confianza cero, que es un modelo de seguridad que sigue la máxima "nunca confíe, siempre verifique", es una prioridad para 9 de cada 10 organizaciones.

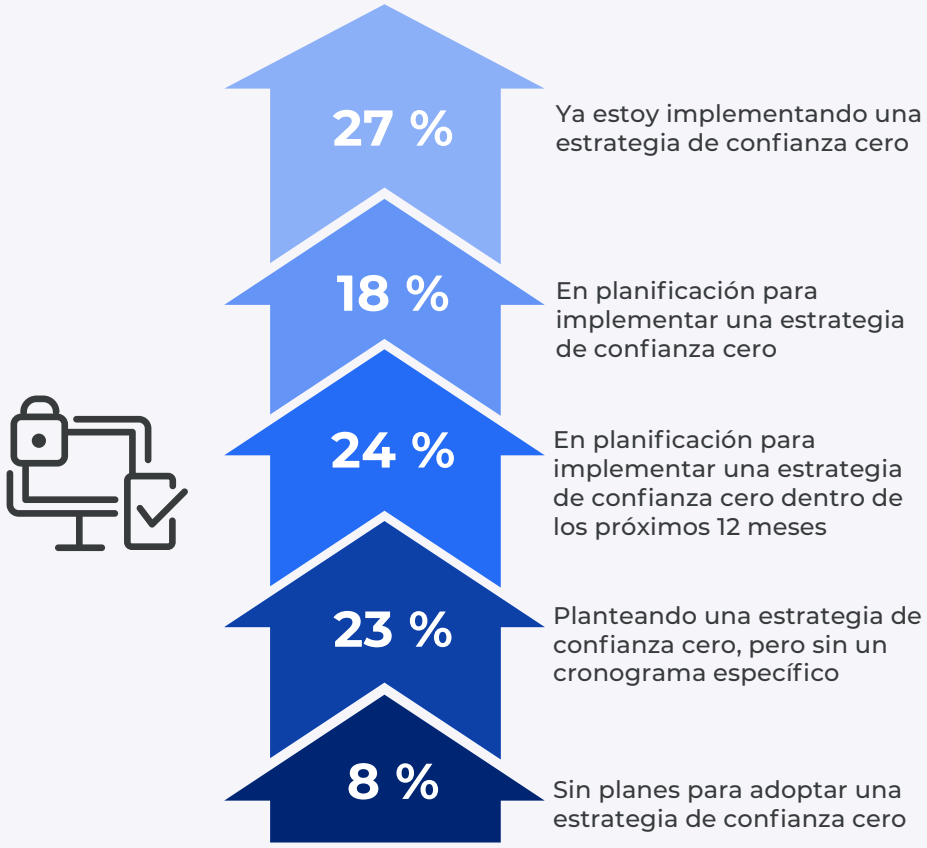
Para aprovechar al máximo una arquitectura de confianza cero, las organizaciones deben priorizar elementos clave como métodos potentes de autenticación multifactor, verificación continua del tráfico, segmentación de la red, acceso con privilegios mínimos y supervisión continua para fortalecer su postura de seguridad.

¿Hasta qué punto es importante adoptar una estrategia de confianza cero para su organización?



Implementar la confianza cero es el objetivo principal

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



El 92 % de las organizaciones ya están implementando (27 %), planeando implementar (42 %) o considerando una estrategia de confianza cero, lo que demuestra que comprenden su importancia y que la confianza cero está pasando de ser una palabra de moda a una realidad para la mayoría de las organizaciones.

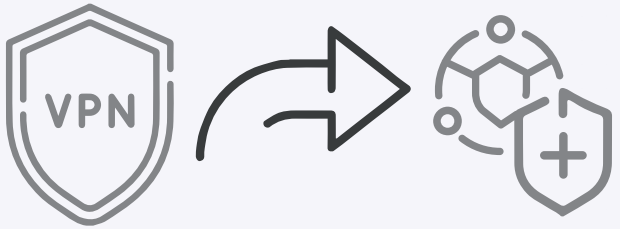
Aquellos que aún no han definido un cronograma para la implementación deberían plantearse acelerar sus planes para seguir siendo competitivos y seguros. Aquellos que no tienen planes o que no están seguros pueden correr el riesgo de quedarse atrás en un panorama de amenazas de seguridad cibernética que evoluciona rápidamente.

Planes de transición de VPN

La transición de las soluciones VPN a Zero Trust Network Access (ZTNA) marca un cambio significativo en las estrategias modernas de seguridad cibernética, dada la prioridad al acceso con menos privilegios y la microsegmentación inherente a ZTNA. 4 de cada 10 organizaciones están haciendo la transición a ZTNA, lo que demuestra una respuesta activa a los requisitos de seguridad en evolución.

Para las organizaciones que planean o están considerando un cambio, es crucial evaluar y elegir soluciones ZTNA que cumplan con sus requisitos de seguridad y necesidades comerciales específicas. Aquellos que actualmente no tienen planes de adoptar ZTNA deberían, como mínimo, investigar los beneficios potenciales de estas soluciones para mejorar su postura de ciberseguridad. Para las empresas que no pueden cambiar por completo, los modelos híbridos pueden ser un compromiso beneficioso, ya que brindan las ventajas de ZTNA y aprovechan la infraestructura VPN existente.

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



El **37 %**

tiene planes para reemplazar VPN con una solución ZTNA en un futuro próximo

Mejores prácticas para su viaje hacia la confianza cero

Recomendamos las siguientes mejores prácticas para realizar con éxito el viaje desde la infraestructura VPN tradicional a una arquitectura moderna de confianza cero.

Evalúe su infraestructura actual:
comience con una revisión exhaustiva de su infraestructura VPN existente. Un 32 % informa de experiencias de usuario deficientes y un 14 % de costes altos, por lo que es crucial comprender sus problemas específicos antes de seguir adelante.

Elija la solución adecuada:
busque una solución de confianza cero que se alinee con sus necesidades únicas. Una solución definida por software y nativa de la nube puede simplificar la gestión, reducir los costes y mejorar la experiencia del usuario, problemas que surgen con frecuencia con las VPN.

Implemente el acceso con privilegios mínimos:
otorgue a los usuarios sólo el acceso necesario a recursos específicos en función de las necesidades de su rol. Este es un elemento fundamental de la confianza cero.

Plan de escalabilidad:
opte por una solución que pueda escalar a medida que crece su empresa. Nuestra encuesta indicó que alrededor del 11 % de las organizaciones se enfrentan a problemas de escalabilidad con sus VPN. Una solución basada en la nube puede manejar de manera efectiva las necesidades de escalabilidad.

Revise y actualice regularmente sus políticas de seguridad:
acostúmbrese a revisar y actualizar constantemente sus políticas de seguridad. Esto ayuda a mantener una postura de seguridad sólida.

Habilite el acceso seguro para todos los usuarios:
adopte una solución que proporcione acceso seguro para empleados remotos, terceros y dispositivos no administrados. Elija una plataforma que sea compatible con cualquier usuario y se pueda usar en cualquier lugar y en cualquier dispositivo.

Supervise y mejore continuamente:
adopte una estrategia de supervisión continua para identificar y responder a posibles problemas antes de que se intensifiquen. La detección y respuesta proactiva de amenazas son clave para una implementación sólida de la confianza cero.

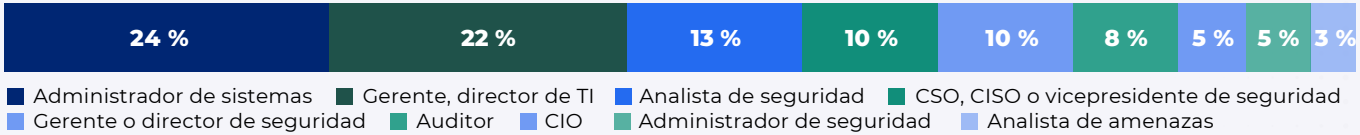
Metodología y demografía

Este informe se basa en los resultados de una exhaustiva encuesta en línea realizada a 382 profesionales de la informática y la ciberseguridad, llevada a cabo en junio de 2023 para identificar las últimas tendencias de adopción por parte de las empresas, los retos, las carencias y las preferencias de soluciones relacionadas con el riesgo de las VPN. Entre los encuestados hay desde ejecutivos técnicos hasta profesionales de seguridad de TI, que representan una sección transversal equilibrada de organizaciones de diferentes tamaños en múltiples sectores.

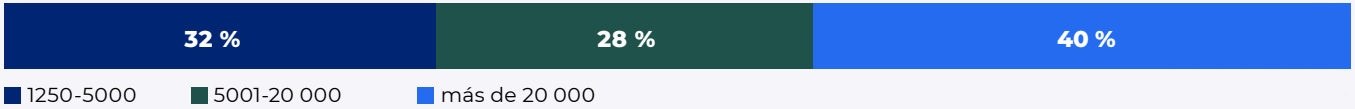
Nivel profesional

Departamento

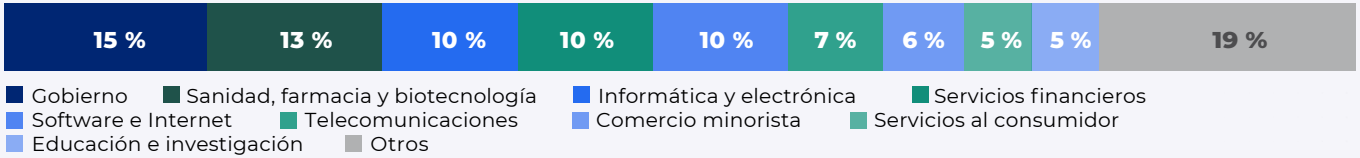
Rol principal



Tamaño de la empresa



Sector



Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de los 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.

Más información en zscaler.es o síganos en Twitter @zscaler.

zscaler.es

Cybersecurity
INSIDERS

Cybersecurity Insiders reúne a más de 600 000 profesionales de seguridad de TI y proveedores de tecnología de clase mundial para facilitar la resolución inteligente de problemas y la colaboración para abordar los desafíos de ciberseguridad más críticos de la actualidad.

Nuestro enfoque se centra en crear y organizar contenido único que eduque e informe a los profesionales de ciberseguridad sobre las últimas tendencias, soluciones y mejores prácticas de ciberseguridad. Desde estudios de investigación integrales y revisiones imparciales de productos hasta guías electrónicas prácticas, seminarios web atractivos y artículos educativos, estamos comprometidos a proporcionar recursos que brinden respuestas basadas en evidencia a los complejos desafíos de ciberseguridad de la actualidad.

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

Envíenos un correo electrónico a **info@cybersecurity-insiders.com** o visite **cybersecurity-insiders.com**