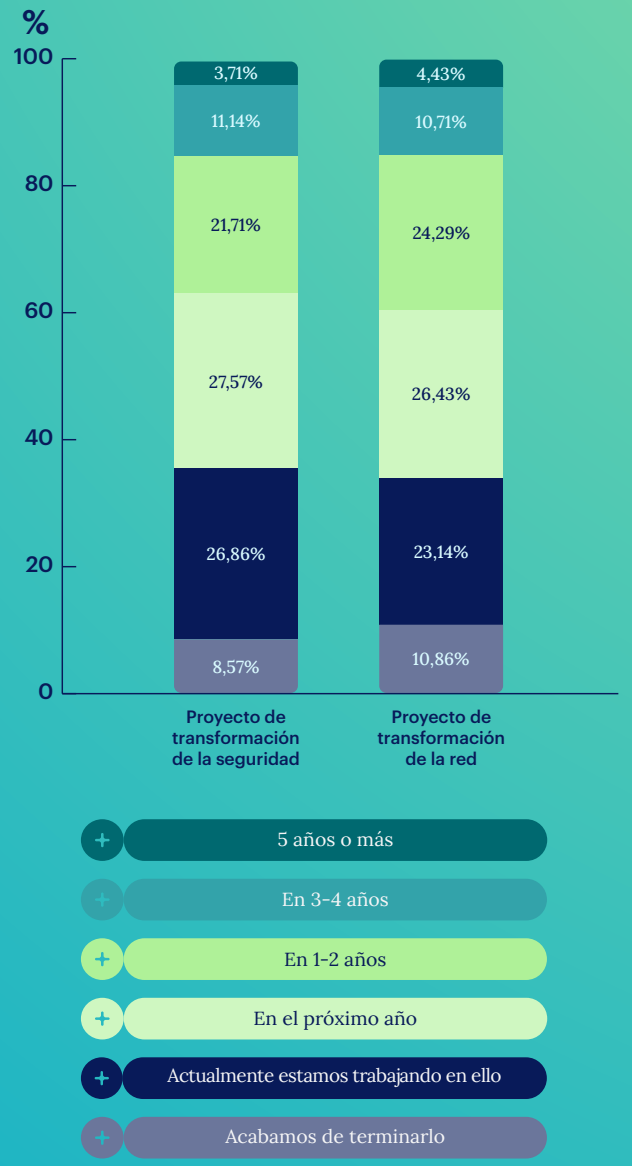

e-book
La transformación de la seguridad y las redes en la era de SASE
netskope

A medida que las organizaciones de todo el mundo continúan con su transformación digital, cada vez son más los recursos operativos que se trasladan a la nube. Estos recursos operativos abarcan todo el parque informático, y el éxito de estos proyectos requiere un replanteamiento tanto de las arquitecturas de las redes como de las de seguridad.

Se prevé que el mercado mundial de transformación de redes alcance los 122 730 millones de dólares en 2026, con una tasa de crecimiento anual compuesta (TCAC) del 39,7%.[1] De forma similar, se prevé que el mercado mundial de seguridad en la nube alcance los 77.500 millones de dólares para ese mismo año a una TCAC del 13,7%.[2]

El cambio está claramente en marcha, pero sigue habiendo poco consenso entre las organizaciones sobre cómo enfocar los proyectos de redes y seguridad en lo que respecta a presupuestos, gestión del cambio o racionalización de la tecnología.

En este libro electrónico se identifican algunos de los principales retos que ha revelado la investigación encargada por Netskope a Censuswide que incluye empresas europeas y que se ha complementado con estudios de terceros para ofrecer una visión global. Nuestro objetivo es comprender mejor cómo los líderes de TI están abordando la transformación en la era de las arquitecturas de servidor perimetral de acceso seguro (SASE) y compartir ideas sobre cómo las organizaciones pueden racionalizar los equipos, los procesos y la tecnología en busca del éxito de SASE.



[1] «Global Network Transformation Market Research Report», Market Research Future, 2021.

[2] «Cloud Security Market Report», MarketsandMarkets, enero de 2022.

El ahorro de costes al trasladar la seguridad a la nube

Según un estudio de Deloitte, la seguridad y la protección de datos son ahora uno de los principales factores que motivan la adopción de la nube en todo el mundo, con un 58% de los ejecutivos de TI que las sitúan en primer o segundo lugar.[3] Por su parte, una encuesta realizada a ejecutivos estadounidenses reveló que la seguridad es considerada la principal ventaja de la informática en la nube por el 60% de los encuestados.[4]

Así lo reflejan nuestras propias investigaciones. La gran mayoría de los directores de información (CIO) y los directores de seguridad de la información (CISO) (98 %) con los que hemos hablado han trasladado parte de sus recursos a la nube, aunque menos de uno de cada cinco (18,5%) ha realizado la transición de más de tres cuartas partes de su infraestructura de seguridad.

La mayoría de los que utilizan la seguridad en la nube ya han reducido el gasto en algunas de las áreas previstas: el 25% ahorra en hardware y el 23% en ancho de banda. Mientras tanto, el 21% ha reducido costes mediante la consolidación de proveedores, y el 21% ha recortado su gasto en dispositivos cortafuegos implementando en su lugar alternativas en la nube. Esto coincide con los hallazgos de estudios de investigación a nivel global. Por ejemplo, un estudio de Secure Data apunta que una empresa con 500 trabajadores reducirá sus gastos en cortafuegos un 37% y ahorrará una media de 139.000 dólares.[5]

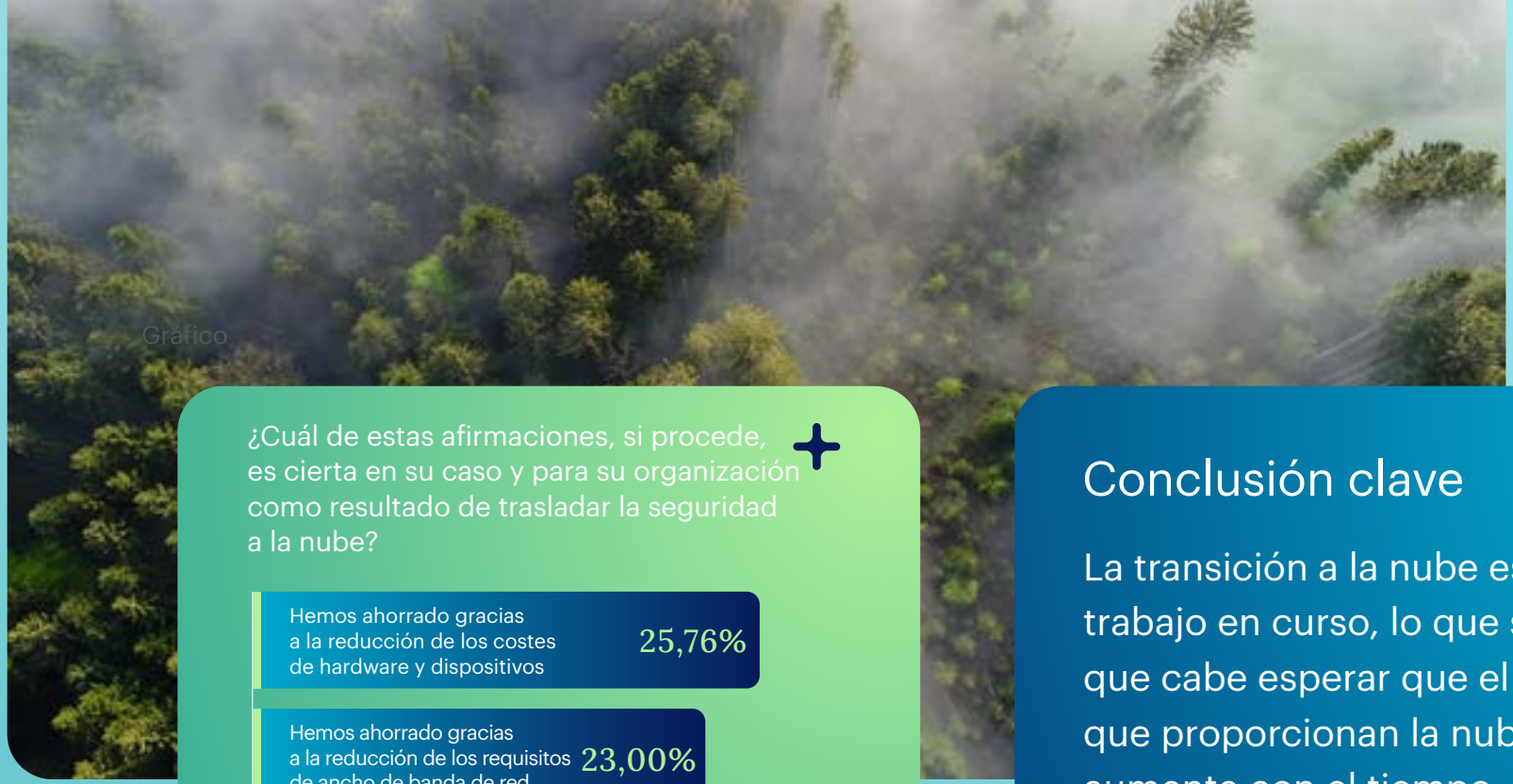
Sin embargo, dado que la mayoría de las empresas aún se encuentran en proceso de transformación digital, es justo considerar estos ahorros de costes reales como preliminares o, al menos, dignos de volver a ser analizados de forma periódica. Por ejemplo, según nuestro estudio, el 30% de los encuestados espera reducir costes mediante la introducción de tecnologías de cortafuegos como servicio (FWaaS), pero solo el 22% afirma haber conseguido este ahorro hasta la fecha.

La seguridad es considerada el principal beneficio de la informática en la nube por el 60 % de los ejecutivos de alto nivel de todo el mundo[6]

La seguridad representará el 6 % del gasto en la nube en 2023[7]

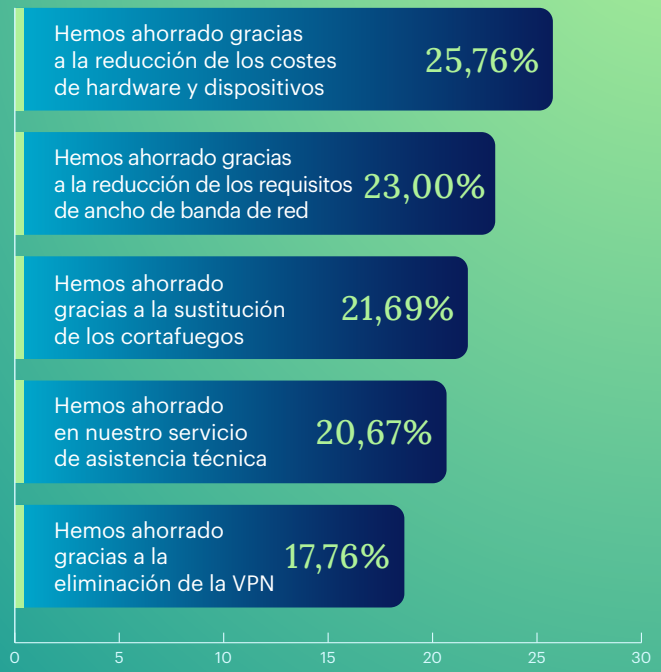
El 98 % de los CIO/CISO europeos han trasladado parte de sus recursos a la nube

Solo el 18,5 % ha trasladado más de tres cuartas partes de su infraestructura de seguridad



Grafico

¿Cuál de estas afirmaciones, si procede, es cierta en su caso y para su organización como resultado de trasladar la seguridad a la nube?



Conclusión clave

La transición a la nube es un trabajo en curso, lo que significa que cabe esperar que el ahorro que proporcionan la nube y SASE aumente con el tiempo.
Las organizaciones se centrarán en proyectos a corto plazo, como la sustitución de la VPN y la consolidación de proveedores, como las mejores formas de ahorro de costes en los próximos uno o dos años.

[3] Karthik Ramachandran y David Linthicum, "Why organizations are moving to the cloud: Security, data modernization, and cost among top drivers for cloud migration," Deloitte, 5 de marzo de 2020.

[4] «55 Cloud Computing Statistics That Will Blow Your Mind», CloudZero, 21 de octubre de 2022.

[5] Abdul Moiz, «12 Reasons to Choose Firewall as a Service for your Business», ExterNetworks, 8 de diciembre de 2022.

[6] «55 Cloud Computing Statistics That Will Blow Your Mind», CloudZero, 21 de octubre de 2022.

[7] Matt Ashare, «Security to take an outsized role in IT spending in 2023», CIO Dive, 4 de octubre de 2022.

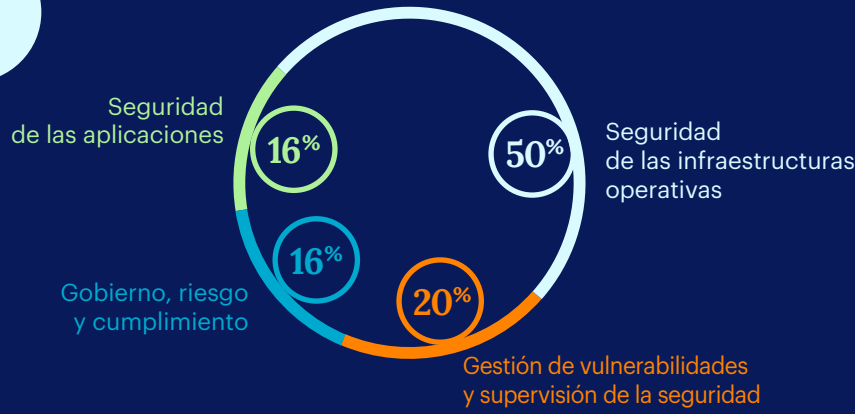
Convergencia de redes y seguridad

Unificar las funciones de seguridad y redes es una práctica recomendada para efectuar el traslado corporativo a la nube. Además, la razón que dieron los encuestados de Netskope para aplicar esta convergencia tiene mucho sentido: aproximadamente un tercio de los CIO y CISO piensan que separar a los equipos no es práctico a la hora de gestionar los recursos de la nube.

Sin embargo, descubrimos que la gran mayoría de las empresas que están fusionando los objetivos de seguridad y redes mantienen separados sus presupuestos. Solo el 8% de los encuestados afirma tener la intención de combinar los presupuestos de seguridad y redes. Aunque ambos equipos estén bajo la supervisión del CIO –alrededor de dos tercios de estos equipos de TI estarán bajo la supervisión tanto del CIO como del CISO, ya sea directamente o a través de jerarquías indirectas– podrían encontrarse compitiendo por los recursos y la propiedad de las tecnologías de la nube; el 28% de los encuestados prevé que ocurrirá exactamente esto.

Esta incertidumbre en torno al enfoque adecuado para crear una estrategia en la nube se refleja en una incertidumbre más amplia sobre la mejor manera de abordar la seguridad en la cúspide de la jerarquía empresarial. Según un estudio global de Economist Intelligence Unit, casi el 40% de los ejecutivos cree que el consejo de administración de la empresa debería supervisar la ciberseguridad, frente al 24% que opina que debería ser una función de un comité cibernético especializado.[8]

Asignación presupuestaria a la ciberseguridad en las empresas[9]



Previsión de inversiones en la red para 2025[10]

50% de las compras de SD-WAN formará parte de una oferta SASE de un único proveedor

10% de las empresas utilizará 5G para la conectividad inalámbrica fija principal o de reserva en su WAN

25% de las empresas automatizará más de la mitad de sus actividades en red

15% de las empresas adoptarán la red como servicio (NaaS) local

30%
de los equipos de seguridad y redes ya se han unido o se unirán,

pero solo el
8%
tiene previsto combinar los presupuestos de seguridad y redes

Conclusión clave

A medida que evolucionan las mejores prácticas de seguridad en la nube, pocas empresas están adoptando un enfoque eficiente óptimo: unir a los grupos de seguridad y redes, tanto desde el punto de vista de la dotación de personal como del presupuesto.

[8] Nick Ismail, «Who is responsible for cyber security in the enterprise?» Information Age, 25 de octubre de 2022.

[9] Toby Shackleton, «Cyber Security Budget Trends in 2022», Six Degrees, 17 de agosto de 2021.

[10] «The top 5 trends in enterprise networking and why they matter: A Gartner® trend insight report», DE-CIX Management GmbH, 22 de septiembre de 2022.

Cuestión de propiedad

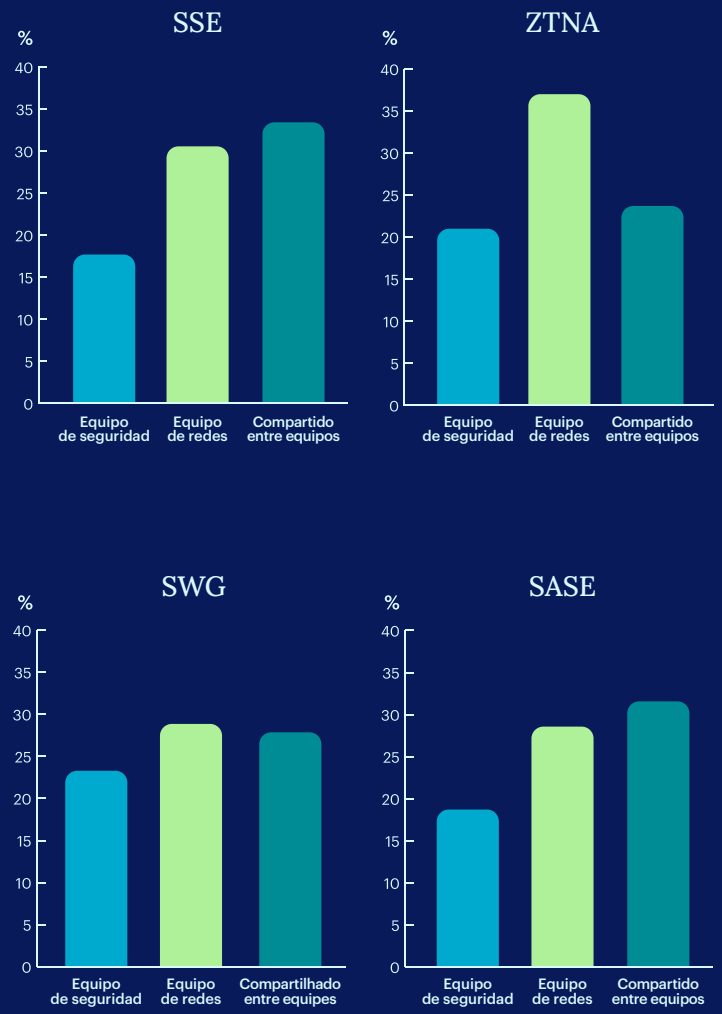
Las tecnologías y los marcos de seguridad transformacionales –incluidos SASE, SSE, ZTNA y SWG– están en el punto de mira de los CIO y los CISO de todo el mundo. Por ejemplo, se espera que el gasto mundial en SASE aumente con una TCAC del 26,4%, hasta alcanzar los 4.100 millones de dólares en 2026.[11] Del mismo modo, se prevé que el gasto mundial total en software y soluciones de seguridad de confianza cero aumente de 27.400 millones de dólares en 2022 a 60 700 millones de dólares en 2027, con una TCAC del 17,3%.[12]

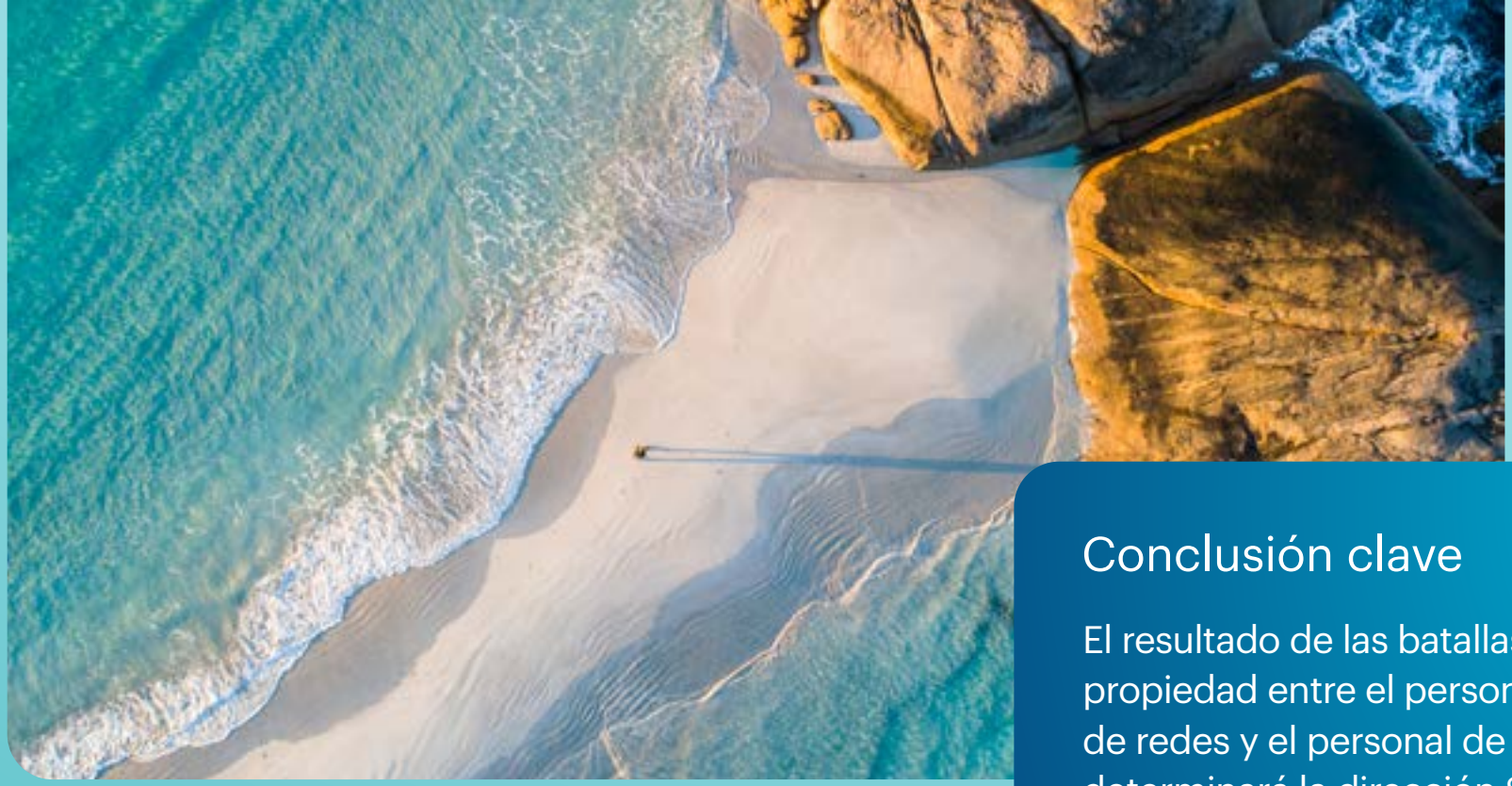
Sin embargo, un interés común por estas tecnologías no se traduce en un acuerdo sobre qué grupo debe tener la propiedad de qué productos o proyectos de transformación. Según nuestra encuesta, el 28% de las empresas confía la responsabilidad de sus proyectos SASE a sus equipos de redes y el 18%, a su organización de seguridad. Mientras tanto, en el 31% de las empresas europeas, la responsabilidad de SASE se comparte entre los dos equipos.

Aunque SSE es un término relativamente nuevo y se considera que comprende los servicios de seguridad que entran en SASE, encontramos divisiones de propiedad muy similares entre ambos. En cuanto a las soluciones SSE, el 30% pertenece al grupo de redes, el 18% pertenece a seguridad, y el 33% son compartidas.

La solución ZTNA se inclina hacia la propiedad de redes (37% de redes frente a 21% de seguridad y 23% compartida). Es ligeramente más probable que SWG sea responsabilidad de un equipo de seguridad que las otras tecnologías (23% de seguridad frente a 28% de redes y 27% compartido).

¿Cuándo tiene previsto su organización emprender un proyecto de transformación de la seguridad o las redes?





Conclusión clave

El resultado de las batallas de propiedad entre el personal interno de redes y el personal de seguridad determinará la dirección SASE de la organización.

Dado que no existe un amplio consenso externo sobre qué equipos son responsables de qué iniciativas, los CIO y CISO deben decidir y ponerse de acuerdo, y después, ser claros y coherentes sobre qué equipo tiene la responsabilidad de cada área de la transformación.

[11] «Secure Access Service Edge Market Report», MarketsandMarkets, agosto de 2021.

[12] «Zero Trust Security Market Report», MarketsandMarkets, agosto de 2021.

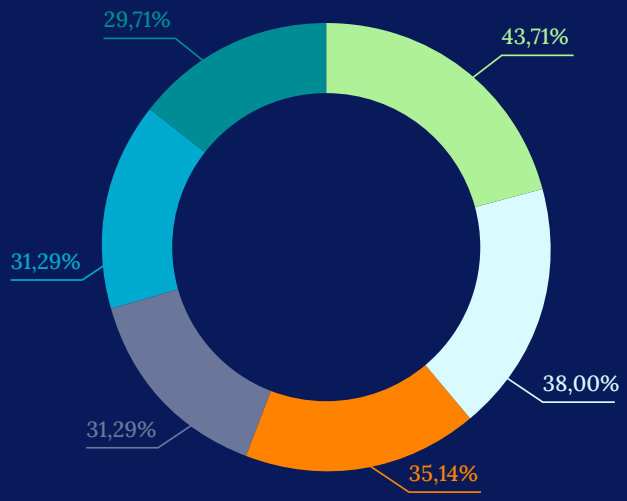
El déficit de competencias en seguridad

Según el informe «Cost of a Data Breach Report 2022» de IBM y Ponemon Institute, el 62% de las organizaciones cree que su equipo de seguridad no cuenta con los recursos suficientes.[13] Nuestra investigación muestra que el paso a la nube tendrá un impacto aún mayor en la dificultad que presenta el déficit de competencias, ya que casi un tercio de los encuestados está ampliando, o espera ampliar, su equipo de seguridad para reflejar el cometido más amplio del grupo a medida que la organización amplía sus operaciones en la nube.

Una proporción significativa de los CIO y CISO encuestados (29%) afirmó no haber tenido problemas para encontrar candidatos cualificados para estos puestos de seguridad. Sin embargo, un grupo aún mayor (46%) tiene dificultades para encontrar candidatos adecuados o espera tenerlas en el futuro. Tal vez debido a estas preocupaciones, el 38% de los encuestados tiene previsto buscar nuevos miembros para su equipo de seguridad fuera del ámbito de la ciberseguridad o incluso de TI.

Abordar la falta de competencias es una misión crítica, porque hasta que no se resuelva, las empresas corren un mayor riesgo de ser víctimas de un ataque. Según el Foro Económico Mundial, al 59% de las organizaciones de todo el mundo le resultaría difícil responder a un incidente de ciberseguridad debido a la escasez de conocimientos de su equipo.[14] Esto no es de extrañar, ya que solo el 8% de los técnicos del mundo tienen conocimientos y experiencia significativos relacionados con la nube.[15] Por el contrario, las empresas con un equipo de seguridad suficientemente dotado informan de que, en su caso, el coste medio de una violación de datos es inferior a la media.[16]

Si tuviera que contratar a alguien para su equipo de seguridad, ¿dónde buscaría a los nuevos miembros del equipo?



- Buscaríamos candidatos capacitados y con experiencia en la nube/SaaS/IaaS
- Buscaríamos candidatos ajenos al mercado de la TI o cibernética y ofreceríamos formación
- En empresas de la competencia, otras empresas del sector u otras organizaciones similares
- Contrataríamos a graduados
- Subcontrataríamos al equipo
- Ofreceríamos formación a nivel interno a los miembros de los equipos de redes, asistencia técnica y otros

40%

de las organizaciones mundiales coincide en que el principal déficit de competencias está en la seguridad.[17]

28%

ya ha realizado cambios en la estructura o el personal del equipo de redes

26%

ha realizado cambios en el equipo de seguridad

Conclusión clave

Que las empresas estén dispuestas a buscar candidatos que aún no tengan conocimientos y experiencia en seguridad en la nube demuestra un nivel de creatividad alentador. Pero no solo es creativo, sino también necesario dada la dificultad que tienen las organizaciones para encontrar talento. Los CIO y CISO que están abiertos a formar a nuevos miembros de los equipos de seguridad–y que están dispuestos a encontrar competencias compatibles o a cultivar talentos preparados en lugares poco tradicionales– tienen muchas menos probabilidades de enfrentarse a una escasez de talento.

[13] «Cost of a Data Breach Report 2022», Ponemon Institute and IBM Security, julio de 2022.

[14] «What you need to know about cybersecurity in 2022», World Economic Forum, 18 de enero de 2022.

[15] «State of Cloud: The cloud skills vs. expectation gap», Pluralsight, 2022.

[16] «Cost of a Data Breach Report 2022», Ponemon Institute and IBM Security, julio de 2022.

[17] «State of Cloud: The cloud skills vs. expectation gap», Pluralsight, 2022.

Presupuestos, personal y reparto de responsabilidades en la era de SASE

Trasladar las operaciones corporativas a la nube representa un verdadero cambio, único en una generación, para las organizaciones de TI y sus CIO y CISO. Como cualquier cambio importante, es probable que la transformación digital resulte incómoda, pero es algo a lo que las organizaciones están dando prioridad. Al mismo tiempo, están transformando las redes y la seguridad al trasladar los sistemas clave a la nube.

Muchas organizaciones todavía están tanteando el camino hacia las mejores prácticas con métodos de prueba y error. Algunas se trasladan a la nube utilizando las mismas estructuras de gestión que funcionaban bien a nivel local con la esperanza de que todo vaya bien. Este planteamiento es arriesgado. No tiene sentido esperar que los conjuntos de competencias y las estrategias presupuestarias heredadas funcionen igual de bien en la nube que en el centro de datos corporativo.

Los líderes que probablemente estén mejor preparados para la transformación digital se están preparando para estos proyectos reajustando los presupuestos, replanteando los recursos de los equipos y reconsiderando las prácticas de captación de personal. Estas organizaciones estarán bien situadas para aprovechar las oportunidades que ofrece una nueva era en que las empresas priorizan el SASE.

Acerca de Netskope

Netskope, líder en servidores perimetrales de acceso seguro (SASE), está redefiniendo la seguridad de la nube, los datos y la red para ayudar a las organizaciones a aplicar los principios de confianza cero.
La plataforma Netskope Intelligent Security Service Edge (SSE) es rápida, fácil de usar y protege a las personas, los dispositivos y los datos en cualquier lugar. Netskope ayuda a las organizaciones a reducir el riesgo, acelerar el rendimiento y obtener una visibilidad inigualable de cualquier actividad en la nube, la web y las aplicaciones privadas.

Miles de clientes, entre los que se encuentran más de 25 empresas de la lista Fortune 100, confían en Netskope y en su potente red NewEdge para hacer frente a las amenazas y los cambios tecnológicos, organizativos, de red y los nuevos requisitos normativos.

Metodología

Investigación realizada en octubre de 2021 por Censuswide por cuenta de Netskope, en la que se llevó a cabo una encuesta a 700 profesionales de TI de Alemania y el Reino Unido. Todos los participantes son CIO, CISO o directores de TI de organizaciones con más de 5000 usuarios de TI.

netskope