netskope

Administrando el cambio: El impacto operativo de la transformación de la red y la seguridad

Presupuestos, personal y división de responsabilidades en la era SASE

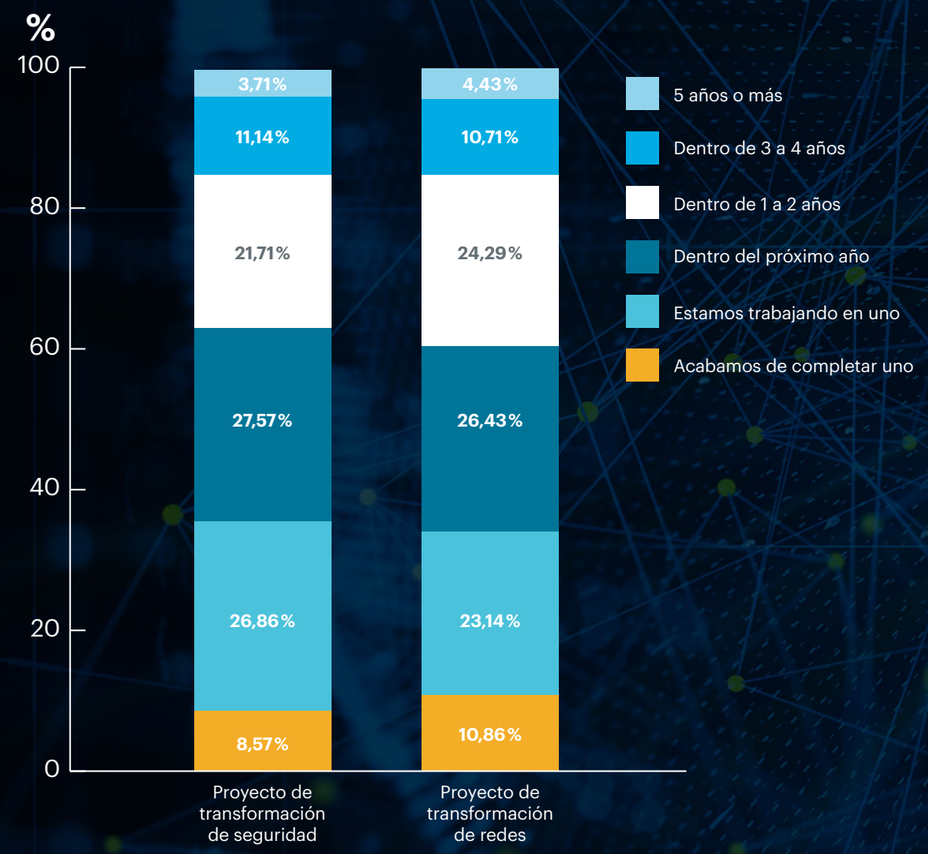
Al igual que las empresas en los demás rincones del mundo, las organizaciones europeas están trasladando cada vez más recursos operativos a la nube, a medida que implementan la transformación digital. El éxito definitivo implica replantear los enfoques tanto de redes como de seguridad; y más del 99,5 % de los equipos de TI en Europa se encuentran ya sea planificando, lanzando o trabajando en proyectos de transformación en estas áreas. Sin embargo, en la actualidad, existe poco consenso entre las organizaciones sobre cómo encarar dichos proyectos, ya sea en cuestión de presupuestos, gestión del cambio o racionalización de la tecnología.

Para poder identificar las mejores prácticas entre estrategias de transformación tan divergentes, Netskope recurrió a Censuswide para que investigara y evaluara las estrategias de redes y de seguridad basadas en la nube, a fin de comprender cómo están abordando la transformación los líderes de TI de las empresas europeas.

Nos encontramos en la era de las arquitecturas Secure Access Service Edge (SASE), donde convergen las redes y la seguridad tanto en los equipos como en las soluciones. Pero nuestra investigación muestra que las empresas están tomando diferentes caminos en sus intentos de transitar esta transformación. En la mayoría de las organizaciones, los equipos de seguridad y de redes mantienen presupuestos separados y responsabilidades definidas. Y, en muchos casos, no queda claro qué equipo es propietario de importantes estrategias o proyectos en la nube.

Este eBook identifica algunos de los retos clave que nuestra investigación ha puesto en evidencia. También sugiere oportunidades de encontrar un enfoque más colaborativo y eficaz para crear operaciones basadas en la nube más seguras y para racionalizar los equipos, los procesos y la tecnología en el camino hacia SASE.

¿Cuándo tiene previsto su organización llevar a cabo un proyecto de transformación de redes y/o seguridad?



El 79 % de los CIO y los CISO ya han apreciado ahorros al trasladar la seguridad a la nube.

La gran mayoría de los CIO y CISO europeos (98 %) ha llevado al menos algunos recursos a la nube, aunque menos de uno de cada cinco (18,5 %) ha trasladado más de tres cuartos de su infraestructura de seguridad. La mayoría de quienes utilizan seguridad en la nube ya han reducido sus gastos en algunas áreas previsibles: El 25 % está ahorrando en hardware y el 23 % en ancho de banda. Mientras tanto, el 21 % ha reducido sus costos al consolidar proveedores, y el 21 % ha recortado sus gastos en appliances de firewall al cambiarlos por alternativas en la nube.

Dado que la gran mayoría de los encuestados aún se encuentra en el proceso de transformación digital, lo justo es considerar estos ahorros como preliminares o al menos considerar reanalizarlos periódicamente. Por ejemplo, el 30 % de los encuestados espera reducir sus costos a través de la introducción de tecnologías Firewall-as-a-Service (FWaaS), pero solo el 22 % afirma haber logrado esos ahorros hasta ahora.

98%

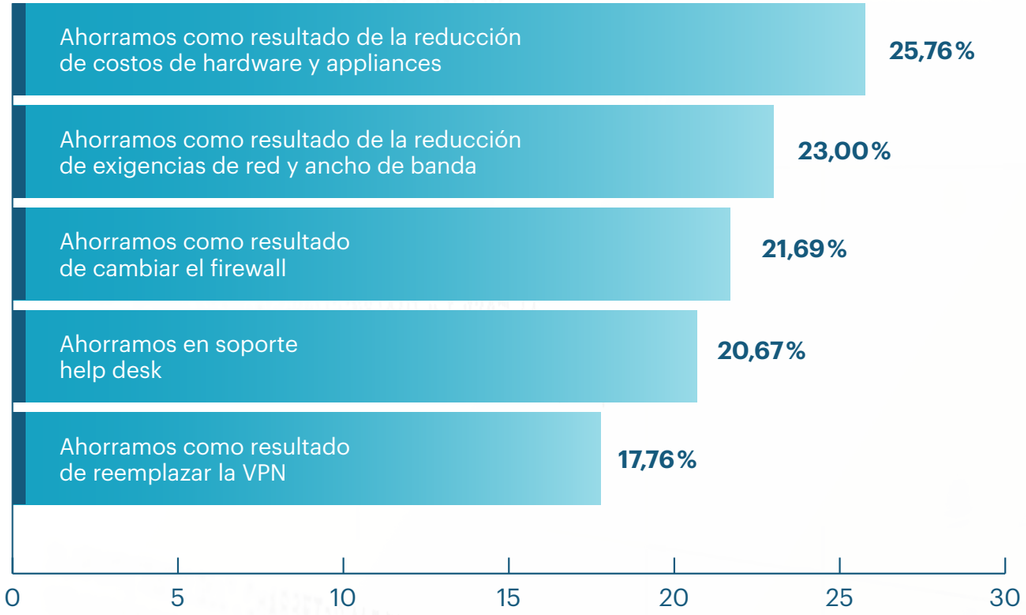
de los CIO/CISO europeos han llevado al menos algunos recursos a la nube

pero solo

18,5%

ha trasladado hasta ahora más de tres cuartos de su infraestructura de seguridad

¿CUÁL DE ESTAS AFIRMACIONES ES APLICABLE A USTED Y SU ORGANIZACIÓN COMO RESULTADO DE TRASLADAR LA SEGURIDAD A LA NUBE?



Conclusión clave

La transición hacia la nube es una labor en curso. Esto quiere decir que se espera que los ahorros que brindan SASE y la nube aumenten con el paso del tiempo. Las empresas se concentran en proyectos a corto plazo —por ejemplo, el reemplazo de las VPN y la consolidación de los proveedores— como las mejores formas de ahorrar costos durante los próximos dos a tres años.

Uno de cada tres CIO o CISO planea unir sus equipos de redes y de seguridad, pero pocos prevén combinar sus presupuestos de redes y de seguridad.

Juntar las funciones de redes y de seguridad es una de las mejores prácticas para el viaje corporativo a la nube. Además, el motivo expresado por los encuestados en cuanto a esta unión tiene muchísimo sentido: Aproximadamente un tercio de los CIO y CISO piensa que separar los equipos no ayuda en la gestión de los recursos en la nube.

Sin embargo, descubrimos que una gran mayoría de las empresas europeas que están unificando su personal de redes y de seguridad mantienen los presupuestos separados. Solo el 8 % de los encuestados dijeron que tienen la intención de combinar sus presupuestos de redes y de seguridad. Incluso si ambos equipos responden ante el CIO (cerca de dos tercios de los equipos de TI europeos responden tanto al CIO como al CISO, ya sea directa o indirectamente), podrían encontrarse compitiendo por los recursos y la propiedad de las tecnologías en la nube; el 28 % de los encuestados prevén precisamente eso.

Estas preocupaciones están agudizadas por una gran falta de consenso entre los encuestados sobre cuál es la estrategia correcta en cuanto a la nube. Descubrimos que el 27 % de las organizaciones están trasladando la responsabilidad y los fondos de la seguridad de la red al equipo de seguridad, con la expectativa de que este presupuesto adicional apoye los proyectos de transformación, incluidos ZTNA y SASE. Al mismo tiempo, otro 27 % está asignando los presupuestos de seguridad a los equipos de redes e infraestructura para financiar un enfoque de security-by-design.

30 %

de los equipos de redes y de seguridad ya se han unido o piensan hacerlo

pero solo el

8 %

planea combinar los presupuestos de seguridad y redes

Conclusión clave

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

Puntos de vista discordantes sobre quién es responsable de las tecnologías clave de seguridad dan paso a luchas por la propiedad.

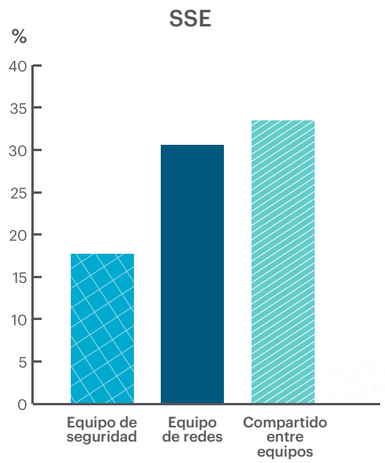
Los marcos y las tecnologías de seguridad transformacionales —entre ellas SASE, SSE, ZTNA y SWG— están en el radar de muchos CIO y CISO europeos. No obstante, un interés en común en estas tecnologías no implica un acuerdo sobre qué grupo debe encargarse de qué productos o proyectos de transformación.

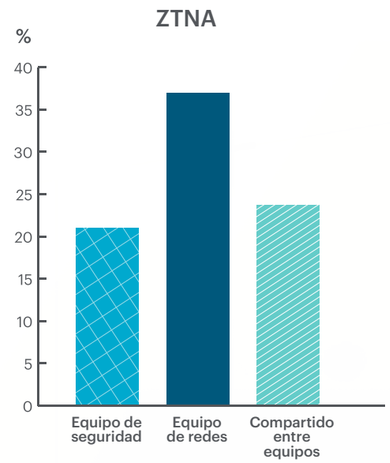
Nuestra encuesta reveló que el 28 % de las empresas otorga la propiedad de sus proyectos de SASE a sus equipos de redes y el 18 % a su departamento de seguridad. Mientras tanto, en el 31 % de las empresas europeas, los dos equipos comparten la responsabilidad por SASE.

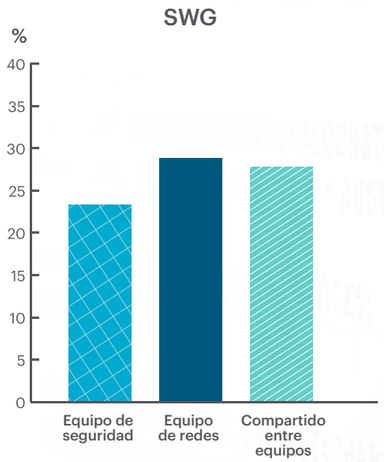
Si bien SSE es un concepto relativamente nuevo y se considera que abarca los servicios de seguridad que integran SASE, nos encontramos con divisiones muy similares de propiedad entre ambos. En cuanto a las soluciones de SSE, el 30 % son propiedad del grupo de redes, el 18 % del de seguridad y el 33 % son compartidas.

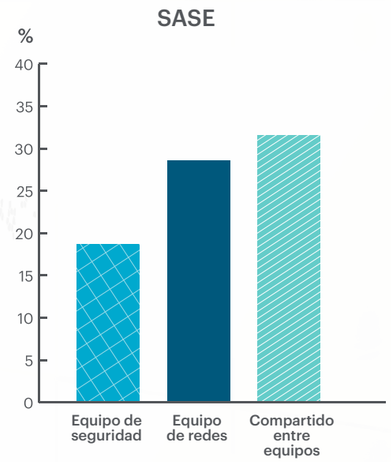
ZTNA se inclina a ser propiedad de redes (37 % redes contra 21 % seguridad y 23 % compartido). SWG es un poco más propensa que las otras tecnologías a ser responsabilidad de un equipo de seguridad (23 % seguridad contra 28 % redes y 27 % compartido).

¿DÓNDE SE ENCUENTRA EL PRESUPUESTO PARA LAS SIGUIENTES TECNOLOGÍAS O INICIATIVAS?









Conclusión clave

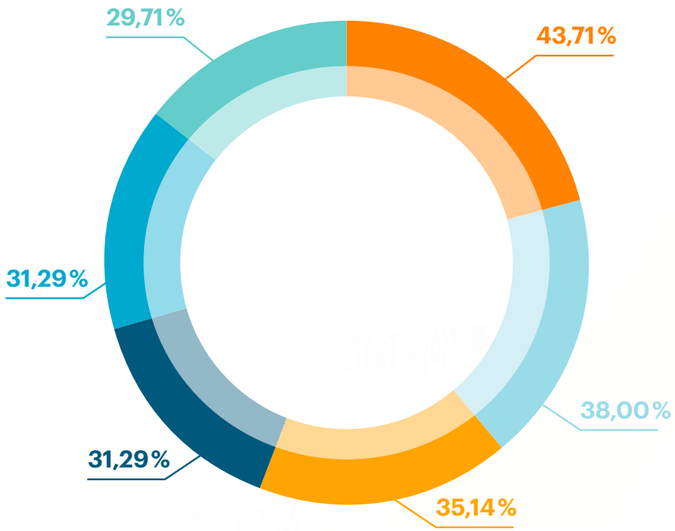
Las luchas por la propiedad entre el personal de redes y de seguridad podrían hacer peligrar los resultados y los beneficios. Dado que no existe un amplio consenso externo sobre qué equipos se encargan de qué iniciativas, el CIO y el CISO deben decidir y ponerse de acuerdo, y luego ser claros y coherentes sobre qué equipo es responsable de cada área de la transformación.

El 46 % de las empresas se enfrenta a un reto a la hora de contratar más personal de seguridad.

Entre las organizaciones europeas que han trasladado algunas actividades de seguridad a la nube, el 28 % ya ha modificado la estructura o el personal del equipo de redes, y el 26 % ha modificado el equipo de seguridad. Casi un tercio de los encuestados se encuentra ampliando, o espera ampliar, su equipo de seguridad para reflejar la mayor jurisdicción del grupo a medida que la organización expande sus operaciones en la nube.

Una importante proporción de los CIO y CISO encuestados (29 %) afirmaron no haber tenido problemas al encontrar candidatos calificados para estos puestos de seguridad. Sin embargo, un grupo aún mayor (46 %) está teniendo dificultades para encontrar candidatos idóneos o espera tenerlas al hacerlo en el futuro. Quizás debido a estas inquietudes, el 38 % de todos los encuestados piensa buscar nuevos integrantes para su equipo de seguridad por fuera del sector de ciberseguridad, o incluso TI.

SI LLEGA A NECESITAR PERSONAL PARA SU EQUIPO DE SEGURIDAD, ¿DE DÓNDE PREVÉ CONTRATAR A LOS NUEVOS INTEGRANTES?



- Buscaríamos candidatos que tengan experiencia y aptitudes en nube/SaaS/IaaS
- Buscaríamos candidatos fuera del área informática y los capacitaríamos/reentrenaríamos
- Nuestra competencia, colegas del sector o de organizaciones similares
- Contrataríamos graduados universitarios
- Subcontrataríamos el equipo
- Reentrenaríamos personal de redes, help desk y otros equipos de forma interna

28% ya ha modificado la estructura o el personal del **equipo de redes**.

26% ha modificado el **equipo de seguridad**.

Conclusión clave

La inclinación de las empresas europeas por buscar candidatos que aún no cuentan con aptitudes y experiencia en seguridad en la nube demuestra un nivel de creatividad alentador. Pero no se trata solo de creatividad, sino también de necesidad: los porcentajes de la encuesta sugieren que a más de dos tercios de los equipos se les dificulta encontrar profesionales. Los CIO y CISO que están dispuestos a capacitar a nuevos integrantes de su equipo de seguridad —y a encontrar idoneidad de aptitudes o candidatos listos para recibir formación en lugares poco convencionales— tienen muchas menos probabilidades de afrontar una escasez de profesionales.

Lo que puede hacer hoy mismo

Trasladar las operaciones corporativas a la nube representa para las organizaciones de TI y sus CIO y CISO un verdadero cambio de paradigma que solo se da una vez en una generación. Al igual que cualquier otro cambio profundo, la transformación digital podría resultar incómoda, pero es algo que las organizaciones están priorizando. Más de la mitad de nuestros encuestados planean poner en marcha sus proyectos de transformación digital dentro de los próximos dos años.

Los CIO y CISO que tienen por delante el mismo plazo para la transformación de redes y de seguridad se enfrentan a una variedad de enfoques opuestos sobre cuál es el mejor camino a seguir. Como lo indica nuestra investigación, la mayoría de las empresas europeas aún están tanteando las mejores prácticas a través de un proceso de prueba y error. Algunas se trasladan a la nube usando las mismas estructuras administrativas que sirvieron in-situ y confiando en que todo salga bien.

Este enfoque es arriesgado. No tiene sentido esperar que las aptitudes y las estrategias presupuestarias de antaño 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 organizando para estos proyectos al realinear los presupuestos, repensar los recursos de equipos y reconsiderar las prácticas de contratación.

Acerca de Netskope

Netskope, el líder en SASE, conecta a los usuarios de modo rápido y seguro directamente a internet, cualquier aplicación y su correspondiente infraestructura, desde cualquier dispositivo, dentro o fuera de la red. Con CASB, Cloud Firewall, SWG y ZTNA integrados de modo nativo en una sola plataforma, Netskope Security Cloud brinda el contexto más granular, mediante tecnología patentada, para permitir acceso condicional y concientización de usuarios, a la vez que impone principios zero trust en la protección de datos y la prevención de amenazas, sea donde sea. A diferencia de quienes fuerzan compromisos entre seguridad y redes, la nube privada de seguridad a nivel mundial de Netskope proporciona funcionalidades computacionales completas en el perímetro.

Netskope ofrece velocidad en cualquier lugar, está centrada en los datos y es cloud-smart, a la vez que permite una buena ciudadanía digital y brinda un costo total de propiedad más bajo.

netskope.com

Metodología

Investigación realizada en octubre de 2021 por Censuswide en representación de Netskope con una encuesta a 700 profesionales de TI en Alemania y el Reino Unido. Los participantes fueron CIO, CISO o directores de TI de organizaciones con más de 5000 usuarios de TI.