El puente a lo posible

Informe de tendencias globales en redes para 2022

Edición especial: el estado del SASE y el auge de la red como servicio (NaaS)

Edición especial: El estado del SASE

Contenido

Adopción de una estrategia de perímetro de servicio de acceso seguro (SASE)

El trabajo híbrido demanda una estrategia de SASE cohesiva para ofrecer una experiencia del usuario excepcional desde cualquier lugar.

Con el fin de abordar el interés y la confusión crecientes en el mercado en torno al perímetro de servicio de acceso seguro (SASE), creamos este apéndice especial para el Informe de tendencias globales en redes para 2022: El auge de las redes como servicio (NaaS).

Impulsado por el fuerte aumento del trabajo remoto y la adopción de la nube híbrida, el SASE (se pronuncia "sasi") proporciona una conectividad segura y sin inconvenientes para cualquier aplicación, sobre cualquier red y desde cualquier ubicación o dispositivo.

El SASE integra funciones de redes y seguridad en una solución o servicio unificado y nativo de la nube.

A diferencia de las soluciones de seguridad tradicionales, acerca las políticas de seguridad y el cumplimiento reglamentario a los usuarios finales y las aplicaciones que están cada vez más distribuidas. Se expande sobre zero trust y elimina la necesidad de retornar los datos a un centro de datos de manera constante, de modo que efectivamente reduce las cargas de red y las barreras, además de ofrecer una experiencia del usuario de calidad superior.

Como alternativa a una pila de seguridad tradicional, proporciona acceso seguro de perímetro a perímetro, lo que cubre los centros de datos, las oficinas remotas, los usuarios de servicio de itinerancia y más.

Este apéndice destaca la información y las tendencias más recientes en torno al SASE, con datos de varias encuestas de mercado y perspectivas sacadas de analistas y expertos prominentes en el sector. Esperamos que esta información lo ayude a entender mejor los beneficios y las implicancias del SASE al momento de formular estrategias para la red, la seguridad y la nube.

— Omri Guelfand, vicepresidente, servicios de redes, Cisco

> "La confusión sobre qué representa SASE aún reina en el mercado. Sin embargo, el consenso emergente se condice correctamente con nuestra perspectiva vigente de que el SASE no es una tecnología nueva, sino una integración de redes existentes, como la WAN definida por software (SD-WAN), y tecnologías de seguridad, como los puertos web seguros (SWG), dentro de una solución de conectividad segura basada en la nube".
>
> — Dell'Oro Group[1]

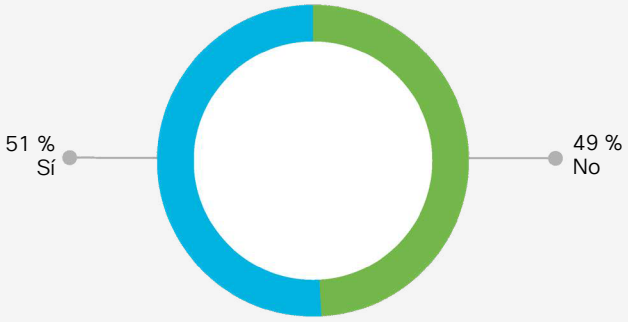
El desafío de la TI: cómo ofrecer una experiencia de trabajo híbrido segura que prioriza la nube

Las dos mayores tendencias con las que los equipos de TI lidian hoy en día son innegablemente la continua transición a una estrategia de aplicación multinube y la adopción de modelos de trabajo híbrido. Con los usuarios y las aplicaciones más distribuidos que nunca, la complejidad para conectarlos y protegerlos se incrementó drásticamente.

La distribución de aplicaciones entre varias nubes públicas y privadas ahora se amplifica debido a la enorme distribución de trabajadores y espacios de trabajo producto del trabajo híbrido. Con esta hiperdistribución, el desafío de tratar de mantener una experiencia del usuario inclusiva y de alta calidad hace un contraste radical con el alguna vez sumamente controlable entorno empresarial dentro de las instalaciones.

En encuestas recientes, el 76 % de los equipos de TI dijo que los trabajadores remotos son más difíciles de proteger, [2] y el 51 % de las organizaciones dijo que no tuvieron problemas para conectar a los trabajadores con los recursos de la compañía durante los últimos 18 meses.[3]

¿Usted o su compañía tuvieron problemas para mantener a los empleados conectados durante los últimos 18 meses?



La transición en curso de un modelo de aplicación centrado en los centros de datos a un modelo con acceso a internet centrado en la nube obligó a muchos equipos de TI a repensar íntegramente su estrategia de redes. De igual manera, los equipos de seguridad se esfuerzan por ofrecer experiencias del usuario seguras y sin inconvenientes cuando tanto los usuarios como las aplicaciones se encuentran por fuera de las instalaciones, donde son más susceptibles a la exposición accidental o los ataques intencionales.

Esto ayuda a explicar el alto nivel de interés en un modelo de SASE a través de la nube y junta soluciones de red, como la SD-WAN, con soluciones de seguridad en la nube, como el perímetro de servicio de seguridad (SSE) y el acceso de red zero trust (ZTNA).

El SASE busca conectar y proteger a los usuarios y las aplicaciones desde donde sea que se ubiquen o se alojen, lo que ofrece una experiencia del usuario más consistente y más segura en última instancia. También promete tanto reducir los costes de TI y la complejidad como mejorar la flexibilidad y el rendimiento de la red además de la experiencia de la aplicación en última instancia.

> "Durante su ápice en 2020, la pandemia impulsó un aumento de un 450 % en la cantidad de empleados norteamericanos con trabajos remotos a tiempo completo o de manera ocasional, en comparación con la línea de base previa a la pandemia. Si bien las tasas comenzaron a caer, prevemos que, en el largo plazo, las tasas de trabajo remoto se consolidarán en un 200 % por encima de la línea de base previa a la pandemia".
>
> — Dell'Oro Group[4]

Conclusión:

Un personal cada vez más distribuido y diversificado llegó para quedarse. Si se implementa de manera adecuada, el SASE conecta y protege tanto a los usuarios como a las aplicaciones distribuidas, alinea las redes y las políticas de seguridad y reduce la carga, además del riesgo de administración de la red y la seguridad.

La relación entre la SD-WAN y el SASE

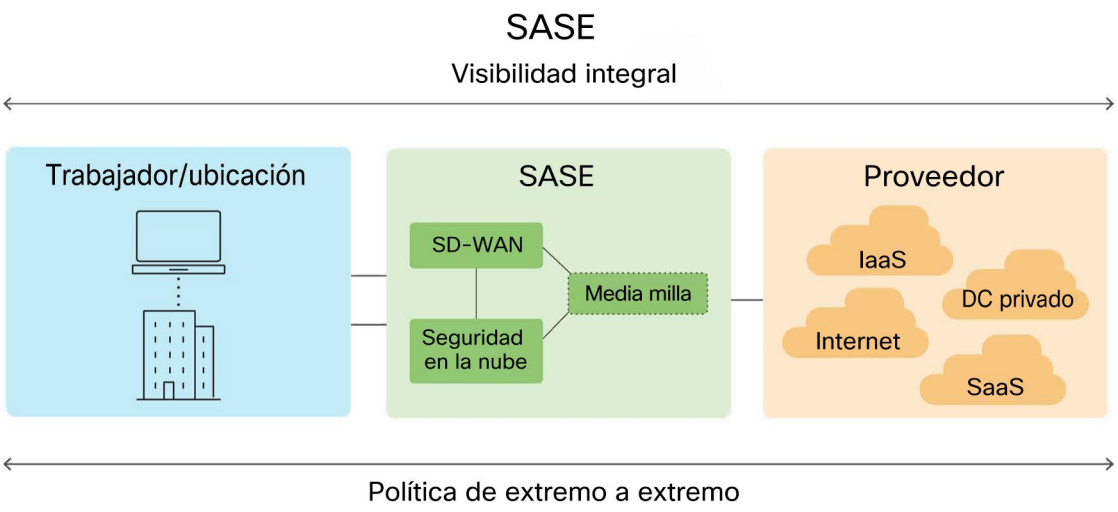
La confusión de mercado en torno al SASE engendró una cantidad de preguntas acerca de las soluciones SD-WAN existentes. ¿El SASE reemplaza a la SD-WAN? ¿Se complementan el uno al otro? ¿O son dos soluciones completamente diferentes para diferentes necesidades?

La respuesta es simple: la SD-WAN es fundamental para el SASE.

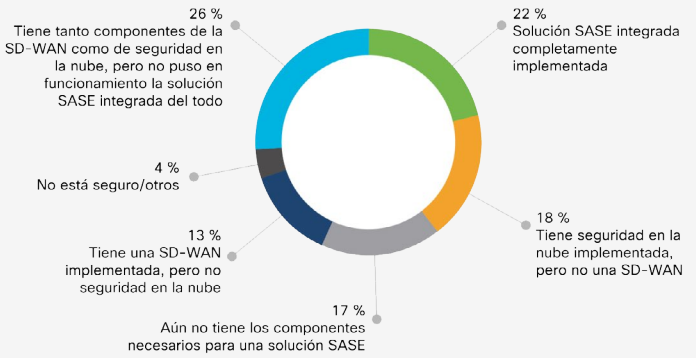
El SASE combina las capacidades de seguridad nativa de la SD-WAN con seguridad centrada en la nube para conectar y proteger a los usuarios y las aplicaciones sin importar dónde se ubiquen o se alojen. Como una arquitectura de superposición, el SASE no puede ofrecer seguridad en todas partes sin las medidas de seguridad que SD-WAN le proporciona, incluidas las siguientes:

- Aprobación de la traducción de direcciones de red (NAT)
- Segmentación de la red en varias subredes
- Monitoreo y bloqueo de malware y de tráfico malicioso
- Restricción de usuarios no autorizados
- Prevención de contenido o aplicaciones no deseados
- Bloqueo por firewall de tráfico entrante y de VLAN a VLAN
- Protección de VPN sitio a sitio o en el túnel
- Geoperimetraje para el control de acceso basado en la ubicación

> "SASE no vuelve obsoleta a la SD-WAN. Sino que la SD-WAN es un componente fundamental del SASE. Las ofertas de SASE son una convergencia de varias redes y capacidades de seguridad como servicio, como la SD-WAN, el puerto web seguro (SWG), el agente de seguridad de acceso a la nube (CASB), el firewall de próxima generación (NGFW) y el acceso de red zero trust (ZTNA)".
>
> — 2021 Gartner®, Quick Answer: Does SASE Replace SD-WAN?[5]



¿En qué etapa de su recorrido de adopción del SASE se encuentra?



Cisco, Encuesta sobre el futuro de la tecnología para 2021, N.° 29 506

¿Cree que las organizaciones de TI deberían comenzar con la SD-WAN o con seguridad en la nube? Muchas personas están adoptando un enfoque por etapas en cuanto a la implementación del SASE. La mayoría de ellas está en el medio de su recorrido con el SASE, con una combinación componentes de la SD-WAN y de seguridad en la nube que aún deben integrarse o ponerse en funcionamiento del todo.

El 18 % de las compañías tienen seguridad en la nube pero no una SD-WAN y el 13 % tienen SD-WAN pero no seguridad en la nube.[6]

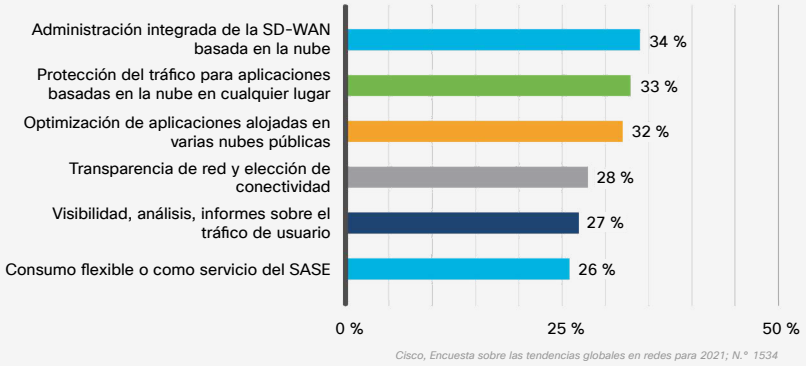
Conclusión:

La SD-WAN es un elemento fundamental del SASE que trabaja codo a codo con soluciones o servicios de seguridad centrados en la nube para proteger a los usuarios y los datos a través de los dominios del perímetro, las instalaciones y la nube.

Expectativa de las capacidades del SASE

Dado que el SASE representa la integración de capacidades de red y seguridad, el 34 % de las organizaciones priorizan las soluciones y los servicios que ofrecen una administración de la SD-WAN integrada y basada en la nube. La protección del tráfico para las aplicaciones basadas en la nube (33 %), la optimización de aplicaciones alojadas en varias nubes públicas (32 %) y la mejora de la transparencia y la flexibilidad de la red (28 %) también se mencionaron como prioridades máximas.

En su opinión, ¿qué capacidades del SASE serían una prioridad para su organización?



Cisco, Encuesta sobre las tendencias globales en redes para 2021; N.° 1534

Para conectar con trabajadores remotos:

El 43 % de las organizaciones planea usar una VPN como servicio.

El 36 % busca adoptar capacidades de acceso de red zero trust y de autenticación de varios factores.

El 35 % está interesado en clientes unificados basados en host.

El 35 % busca extender su SD-WAN a dispositivos móviles y usuarios domésticos.

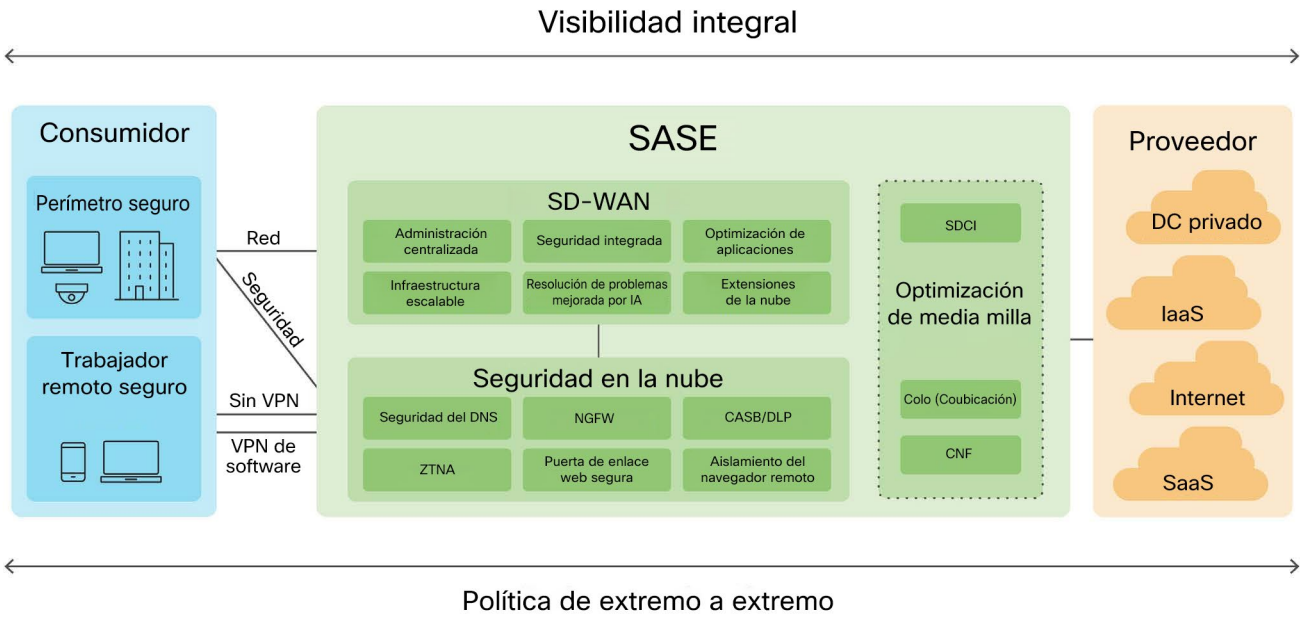
Si bien las arquitecturas, las soluciones y los servicios del SASE siguen evolucionando, estos están fundamentalmente diseñados para unir algunas o todas las capacidades centrales que proporcionan la SD-WAN y la seguridad en la nube:

SD-WAN	Seguridad en la nube
Administración centralizada Un panel centralizado y sumamente visual que facilita la configuración del dispositivo, la administración de redes, el monitoreo y la automatización. Incluye aprovisionamiento automatizado en el perímetro de la red.	**Acceso de red zero trust (ZTNA)** Un marco de seguridad que mitiga el acceso no autorizado contiene las brechas y reduce los movimientos laterales de los atacantes en toda la red. El ZTNA debe emparejarse con una sólida administración de identidad y acceso para verificar la identidad de los usuarios y generar confianza en el dispositivo antes de conceder acceso a aplicaciones autorizadas.
Extensión de red en la nube y optimización de media milla Extensas integraciones de acceso a la nube para permitir una conectividad automatizada y sin inconvenientes con cualquier configuración de sitio a nube o sitio a sitio. Incluye conectividad de media milla a través de la interconexión de nube definida por software (SDCI) e integraciones de colocación.	**Puerto web seguro (SWG)** Un gateway que registra e inspecciona tráfico web para proporcionar visibilidad completa, filtrado de URL además de control de aplicaciones y protección contra malware.
Experiencia con las aplicaciones La habilidad de monitorear y validar la usabilidad y el rendimiento de aplicaciones web. Las métricas y las cascadas detalladas muestran la obtención y la carga secuenciales de componentes web para identificar tanto errores como obstáculos y entender el impacto en el rendimiento de la aplicación.	**Firewall distribuido a través de la nube con un sistema de prevención de intrusiones (IPS)** Servicios implementados mediante la nube y basados en software que ayudan a administrar e inspeccionar el tráfico de red.
Infraestructura flexible y escalable Una amplia gama de plataformas virtuales y físicas que ofrecen alta disponibilidad y rendimiento, opciones de puerto multigigabit, enlaces celulares 5G y poderosas capacidades de encriptación. Optimiza el tráfico WAN mediante la selección dinámica de los enlaces WAN más eficientes que cumplen con los requisitos al nivel del servicio.	**Agente de seguridad de acceso a la nube (**CASB**)** Un software que detecta e informa sobre las aplicaciones en la nube en uso en toda la red, lo que expone la TI en las sombras y permite el bloqueo de aplicaciones de SaaS riesgosas y acciones específicas, como las publicaciones y las cargas de contenido.
Resolución de problemas mejorada por IA IA/ML robustas para optimizar el rendimiento de la red, automatizar tareas manuales de rutina y acelerar la resolución de problemas. Ofrece una función de notificación inteligente, reparación automática y capacidades predictivas de reenrutamiento a internet.	**Prevención de pérdida de datos (DLP)** Un software que analiza datos en línea para ofrecer visibilidad y control sobre datos confidenciales que se envían o se extraen por fuera de la red o la nube de la organización.
Seguridad integrada Capacidades de seguridad que trabajan codo a codo con seguridad en la nube para proteger a sucursales, usuarios domésticos y aplicaciones basadas en la nube de la infiltración.	**Aislamiento del navegador remoto (RBI)** Un software que aísla el tráfico web de los dispositivos de usuarios para mitigar el riesgo de amenazas a través del navegador.
Administración de políticas basada en identidades Microsegmentación y administración de políticas basada en identidades en varias ubicaciones y dominios.	**Seguridad de capa de DNS** Un software que actúa como primera línea de defensa contra amenazas en internet, bloqueando solicitudes de DNS maliciosas antes de que se establezca una conexión con una dirección IP. Una seguridad de DNS sólida puede reducir en gran medida la cantidad de amenazas que un equipo de seguridad debe evaluar y clasificar cada día.
Información avanzada Una visibilidad mejorada de las aplicaciones, internet, la nube y los entornos de SaaS con análisis integrales de salto en salto. Permite el aislamiento de dominios de errores y proporciona información procesable para acelerar la resolución de errores y minimizar o eliminar el impacto en los usuarios.	**Inteligencia de amenazas** Investigadores de amenazas, ingenieros y científicos de datos que usan telemetría y sistemas sofisticados para crear inteligencia de amenazas precisa, rápida y procesable con el fin de identificar amenazas emergentes, descubrir nuevas vulnerabilidades y prohibir amenazas sueltas antes de que se extiendan, a través de conjuntos de reglas que son compatibles con las herramientas en su pila de seguridad.

Además de integrar capacidades SD-WAN y de seguridad en la nube, los modelos de SASE pueden ayudar a desarmar silos operacionales y a fomentar un mayor alineamiento entre la red y los equipos de seguridad. Con políticas estandarizadas, telemetría compartida, y alertas coordinadas en todos los componentes de seguridad y de red, el SASE permite que los equipos de NetOps y SecOps puedan mejorar la eficiencia, la visibilidad y la protección de la TI.

Con esto en mente, es importante para las organizaciones tener una estrategia SASE integral que acomode tanto los objetivos de NetOps como los de SecOps, aumente el alineamiento operacional y sea capaz de soportar las necesidades de la organización para el futuro próximo.

SASE: detalles



> "Para 2024, el 30 % de las empresas adoptarán las capacidades de puerto web seguro (SWG) a través de la nube, el agente de seguridad de acceso a la nube (CASB), el acceso de red zero trust (ZTNA) y firewall como servicio (FWaaS) para sucursales de un mismo proveedor, hasta desde un 5 % menos que en 2020".
>
> – Gartner[7]

Conclusión:

Mientras evalúan estrategias y ofertas de SASE, las organizaciones buscan soluciones y servicios que ofrezcan capacidades fundamentales tanto de SD-WAN *como* de seguridad en la nube para satisfacer sus necesidades actuales y en desarrollo.

La importancia de la integración

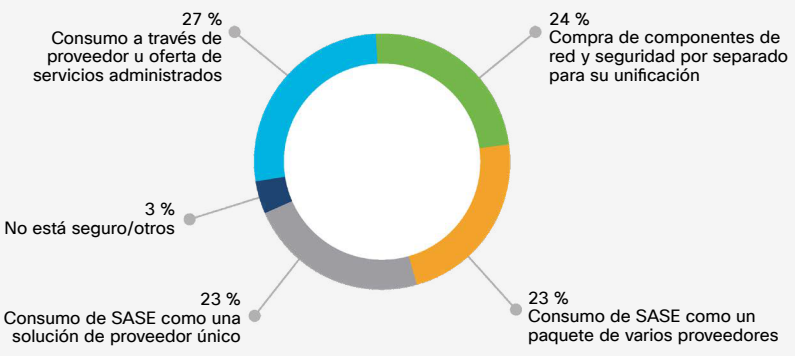
Las empresas modernas dependen de una cantidad de entornos de red (redes de centros de datos, redes de área local, redes de área extensa) y soluciones de seguridad (firewalls, gateways y control de acceso para sistemas basados en la nube y en las instalaciones). A través de las integraciones de tecnologías y de servicios, el SASE puede proporcionar visibilidad, organización de políticas y protección en todos ellos.

Con el objetivo final de conectar a los usuarios y las aplicaciones de manera segura desde donde sea que se ubiquen o se alojen, estas integraciones pueden ayudarle a lograr lo siguiente:

- Reduzca el volumen de incidentes de seguridad.
- Acelere el reconocimiento y la resolución de problemas.
- Simplifique el monitoreo y la administración de sistemas.
- Mejore la ejecución y la estandarización de las políticas.
- Respalde el cumplimiento de las normas regionales y los requisitos de datos.
- Reduzca los costes operativos y de capital.

> "Existen dos tipos importantes de implementaciones de SASE en el mercado, la unificada y la desagregada. La implementación unificada consiste en plataformas SASE, de proveedor único, estrechamente integradas. La implementación desagregada es una implementación que incluye a varios proveedores o varios productos y cuenta con menos integración en comparación con la variante unificada".
>
> – Dell'Oro Group[9]

¿Cómo podrá implementar y poner en funcionamiento su plataforma de SASE?



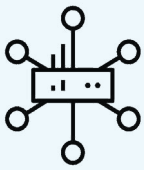
Cisco, Encuesta sobre el futuro de la tecnología para 2021; N.° 29 506

Con el surgimiento de las soluciones y los servicios de proveedor único o de varios proveedores y la posibilidad de las arquitecturas creadas a medida que ensamblan un conjunto de soluciones puntuales, las organizaciones tienen varias opciones para elegir cómo implementar y poner en funcionamiento el SASE.

Dado que construir e integrar una solución personalizada o poner en funcionamiento un paquete SASE de varios proveedores puede dar lugar a complejidades no deseadas, desafíos operacionales y vulnerabilidades de seguridad, muchos (50 %) buscan una solución unificada o administrada de un proveedor único.

- El 70 % está de acuerdo o completamente convencido de que se ha vuelto cada vez más complejo administrar eficientemente una pila de seguridad y una red con varios proveedores.
- El 26 % tiene tanto capacidades de seguridad en la nube como de SD-WAN, pero las puso en funcionamiento y las integró del todo en un modelo de SASE completo.[10]

Ya se trate de una arquitectura creada a medida, un paquete de varios proveedores, un servicio completamente administrado de un solo proveedor o una variación de este, cada solución SASE debe ofrecer un mejor alineamiento e integración entre lo siguiente:



La SD-WAN y la seguridad en la nube

- Automatiza el enrutamiento del tráfico entre el dispositivo SD-WAN y los puntos de presencia (PoP) de seguridad en la nube.
- Redirige automáticamente el tráfico a un PoP alternativo para generar resiliencia cuando hay un problema de rendimiento.
- Utiliza análisis predictivos con acceso a IA para redirigir automáticamente el tráfico a los PoP alternativos antes de que la experiencia del usuario se vea afectada.

Equipos de NetOps y SecOps

- Es capaz de compartir continuamente políticas de seguridad (como autorizaciones de accesos y segmentación) entre la SD-WAN y las implementaciones de seguridad en la nube.
- Permite el intercambio de datos entre la SD-WAN y las plataformas de administración de seguridad en la nube para proporcionar visibilidad a las políticas y los eventos.
- Extiende y propaga las construcciones de redes empresariales (como las VPN y las etiquetas de grupo de seguridad) y las políticas en plataformas de seguridad en la nube.
- Utiliza la autenticación administrativa de inicio de sesión único (SSO) en la SD-WAN y las plataformas de administración de seguridad en la nube.

Usuarios finales y aplicaciones

- Permite la conectividad directa entre los servicios SD-WAN, de media milla (como la SDCI), multinube y de SaaS.
- Monitorea y optimiza la experiencia del usuario con visibilidad y análisis completos a través de la SD-WAN, los PoP de seguridad en la nube y las conexiones de IaaS o SaaS.

"Es imposible crear redes de manera correcta sin integrar seguridad. Necesito ver la seguridad de manera holística, desde el terminal a través de la red hasta la aplicación. Con la red como servicio, necesito que el proveedor se haga responsable de la red y la seguridad. Si solo se hacen responsables de la red, necesito la visibilidad y el control necesarios para garantizar una protección completa y una rápida mitigación de amenazas. En el estado ideal, el proveedor se encargaría tanto de la creación de las redes como de la seguridad correctamente".

– Director de infraestructura de TI, compañía de productos de consumo global

Conclusión:

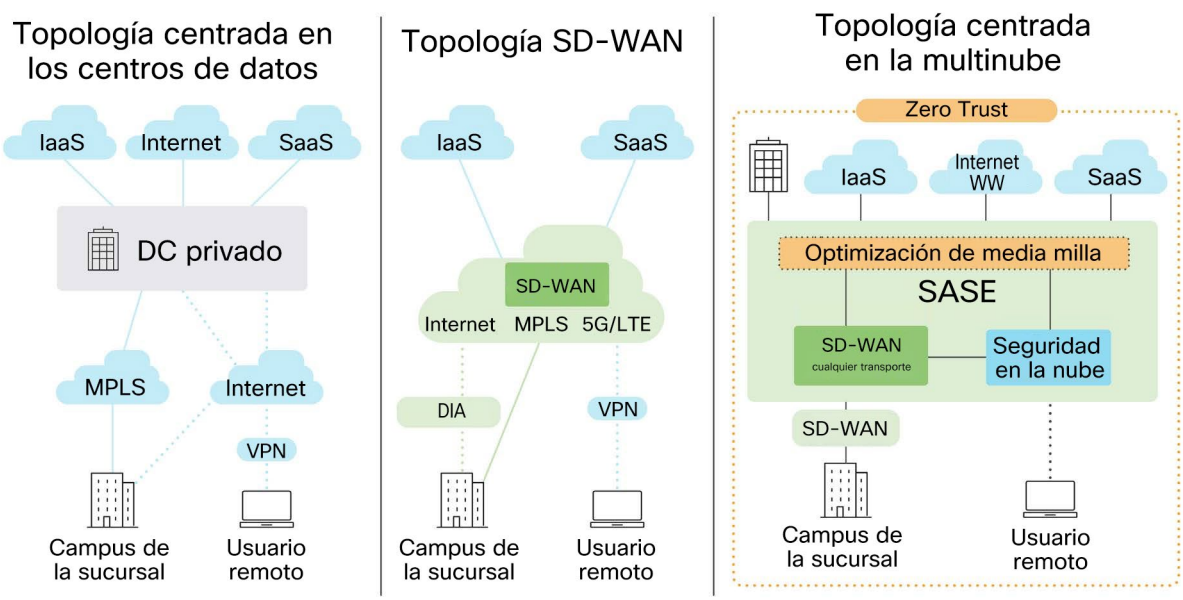
Ya sean creados a medida u ofrecidos por uno o más proveedores, las soluciones y los servicios SASE deben proporcionar una integración estrecha entre la SD-WAN y los sistemas de seguridad en la nube para optimizar una experiencia del usuario segura y la colaboración con NetOps y SecOps.

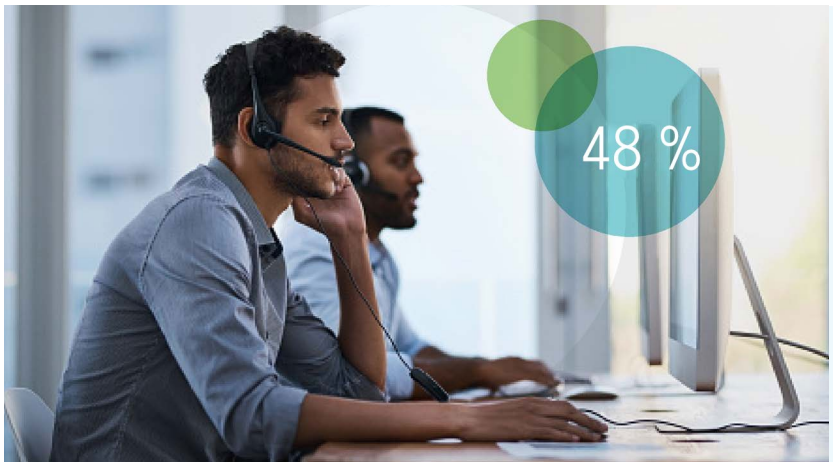
Tendencias de adopción del SASE

Al igual que con cualquier decisión tecnológica, el modelo de SASE y el enfoque de implementación adecuados serán únicos para cada organización. Las soluciones de red y seguridad ya existentes, así como las estrategias operacionales generales y las prioridades de negocio, deben ser factores de impulso en toda decisión de SASE. También deben considerarse las iniciativas críticas, las demandas regulatorias, las fusiones y adquisiciones, las operaciones de cadena de suministro y los requisitos para la resiliencia empresarial.

Las organizaciones que migran de un modelo de aplicación centrado en los centros de datos a un modelo centrado en la nube o multinube pueden comenzar su recorrido SASE con la SD-WAN, por ejemplo, a continuación de la optimización de media milla y la integración de seguridad en la nube.

De una topología centrada en DC a una centrada en la multinube





El 48 % de las compañías interesadas en el SASE comenzará con la seguridad, el 31 % comenzará con la red y el 21 % planea abordar la seguridad y las redes simultáneamente.[8]

Independientemente del modelo particular o el enfoque de implementación, muchas compañías dicen que ya están en marcha con la adopción del SASE: el 86 % de las organizaciones están considerando la adopción o ya adoptaron el SASE.[11]

¿Acaso su compañía adoptó, decidió adoptar o consideró adoptar soluciones SASE?

Cisco, Encuesta sobre el futuro de la tecnología para 2021; N.° 34 351

"Para 2025, al menos el 60 % de las empresas tendrán estrategias y plazos explícitos para la adopción del SASE que abarcarán a el acceso del usuario, las sucursales y el perímetro, hasta desde un 10 % más que en 2020".

– Gartner[12]

Conclusión:

Los enfoques de implementación de SASE están influenciados por los ciclos de vida de la infraestructura existente, las prioridades operacionales y las iniciativas empresariales. Los equipos de TI deben adoptar un enfoque de planificación estratégico que apunte a construir gradualmente una arquitectura SASE completa.

Modelos de consumo del SASE

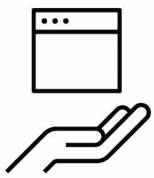
Existen tres modelos de consumo primario para soluciones y servicios SASE. Si bien estos modelos de consumo tienen diferentes impactos en los equipos internos y las operaciones, todos ellos desarman las redes y los silos de seguridad tradicionales. Como resultado, el SASE puede presentarse como una función de forzamiento que mejora el alineamiento operacional y la eficiencia.

Como servicio

Para aquellos que desean una implementación rápida, un impacto mínimo en las operaciones y el riesgo reducido que viene con los SLA, el SASE como servicio les proporciona una gran cantidad de capacidades a través de la nube completamente integradas en un único panel y un soporte durante todo el ciclo de vida. El 26 % de las organizaciones mencionan al SASE como servicio como su modelo de consumo preferido.

Híbrido o administrado de manera conjunta

Las organizaciones que aún no están preparadas para un modelo como servicio completo o que quieren más opciones de personalización de las que esos servicios pueden ofrecer, pueden adoptar un enfoque híbrido. Esto implica integrar capacidades de seguridad basadas en la nube con una solución SD-WAN o compartir las responsabilidades de la red y la seguridad con un proveedor de servicios administrados. Estos enfoques híbridos proporcionan seguridad adicional y soporte además de permitirles a los equipos de TI mantener una medida de visibilidad y control mientras reducen las demandas totales de la administración del ciclo de vida.



Altamente personalizable o DIY

Las organizaciones que desean la personalización y el control completos de su red y su espacio de seguridad pueden crear, integrar y administrar las capacidades del SASE por su cuenta. Este nivel de personalización y control suele ir en detrimento de la velocidad y la agilidad. Esto requiere una administración adicional del ciclo de vida del hardware, el software y las licencias. Además, necesita de especialistas adicionales en seguridad y cumplimiento de las normas. Esta es una buena opción para las organizaciones que tienen demandas muy específicas, así como una red y un personal existentes que pueden cumplir con los requisitos arquitectónicos y operacionales del SASE.

Lea acerca de lo que aprendimos en este Caso de estudio sobre la implementación del perímetro de servicio de acceso seguro (SASE) de Cisco.

Conclusión:

Existen varios modelos de consumo del SASE con impactos operacionales variables. El modelo adecuado para cada organización depende de un número de factores, incluidos el tamaño, el conjunto de habilidades y el ancho de banda del equipo interno de TI, así como la priorización de las necesidades específicas, la velocidad, la agilidad, la visibilidad y el control.

Conclusión sobre el SASE

Las arquitecturas, las soluciones y los servicios SASE proporcionan una conectividad segura entre cualquier usuario y cualquier aplicación, sin importar dónde se ubiquen o se alojen. Pero el recorrido al SASE será único para cada organización. El modelo y el enfoque adecuados dependerán de las inversiones en tecnología existentes así como de las prioridades de TI y empresariales.

Cisco y nuestro ecosistema de partners pueden ayudarle a abordar sus necesidades únicas de red y de seguridad con la solución SASE más completa, flexible y resiliente del mercado.

Puede elegir entre nuestra amplia cartera de SASE que combina las mejores redes de su clase, conectividad del cliente, seguridad y capacidades únicas de observabilidad de internet para ofrecerle los resultados que necesita. También puede elegir entre una gama de modelos de consumo e implementación del SASE simples y flexibles que abordan una variedad de situaciones y requisitos.

Nuestra infraestructura global de seguridad en la nube de alta disponibilidad proporciona un acceso seguro desde donde sea que residan los usuarios y las aplicaciones. Además nuestras soluciones SD-WAN líderes en el mercado proporcionan la agilidad y las funciones necesarias para ofrecerles experiencias de calidad consistentemente alta a sus usuarios. En conjunto, nuestras soluciones SD-WAN y de seguridad en la nube proporcionan las capacidades de SASE más completas e integradas de manera única de la industria.

Para continuar, Cisco está innovando en torno al SASE a un ritmo acelerado a través de integraciones y mejoras de las funciones de manera continua. Estamos desarrollando nuestras ofertas para ofrecer los servicios SASE más flexibles y de fácil consumo para sus términos.

Para obtener más información, visite el Centro de recursos de SASE de Cisco.

Se reconoció a Cisco como líder en infraestructura WAN Edge en Gartner Magic Quadrant™ por su habilidad para ejecutar y la integridad de su visión.[13]

Asistencia y recursos adicionales

Enlace a la hoja de ruta del SASE >

Encuentre un partner de Cisco >

Contáctese con ventas de Cisco >

Fuentes sobre el SASE

1. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, septiembre de 2021.
2. The State of Security 2021, Splunk, febrero de 2021.
3. El futuro de la tecnología, Cisco, noviembre de 2021.
4. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, septiembre de 2021.
5. Gartner Quick Answer: Does SASE Replace SD-WAN?, Andrew Lerner, Neil MacDonald, diciembre de 2021.
6. Informe de tendencias globales en redes para 2022: El auge de la red como servicio, Cisco, octubre de 2021.
7. Gartner 2021 Strategic Roadmap for SASE Convergence, marzo de 2021.
8. SASE Trends: Plans Coalesce but Convergence Will Be Phased, ESG Research Report, diciembre de 2021.
9. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, septiembre de 2021.
10. Informe de tendencias globales en redes para 2022: El auge de la red como servicio, Cisco, octubre de 2021.
11. El futuro de la tecnología, Cisco, noviembre de 2021.
12. 2021 Strategic Roadmap for SASE Convergence, Gartner, marzo de 2021.
13. Gartner Magic Quadrant for WAN Edge Infrastructure, septiembre de 2021.

Informe de tendencias mundiales en redes de 2022

El auge de la red como servicio (NaaS) Informe

Contenido

Bienvenida

Bienvenido al informe *de tendencias mundiales en redes de 2022: El auge de la red como servicio (NaaS)*

Qué tiempos notables estamos viviendo, tanto los humanos como los profesionales de redes. El año pasado, los líderes de TI y los profesionales de redes tuvieron la tarea de habilitar a los trabajadores remotos, proteger los datos en un panorama de computación más distribuido, y prestar nuevos servicios a usuarios, clientes y partners. Muchas empresas aceleraron los esfuerzos de transformación digital a fin de cumplir con los nuevos requisitos, aprovechando la nube y el software como servicio (SaaS) para una mayor flexibilidad, agilidad y velocidad.

En nuestro informe de tendencias mundiales en redes de 2021, resaltamos las formas en que se utilizan las tecnologías de red para mejorar la resiliencia empresarial, independientemente de las circunstancias.

En el informe de este año, nos centramos en una tendencia emergente que tiene muchas consecuencias para el futuro: las redes como servicio.

Siguiendo de cerca a los cada vez más populares modelos como servicio (aaS), por ejemplo, el SaaS y la infraestructura como servicio (IaaS), las NaaS invariablemente cambiarán la forma en que muchas empresas adquieren, entregan y administran las capacidades de la red. Para saber más, hablamos con 20 líderes de TI y encuestamos a 1534 profesionales de TI de de 13 países respecto de cómo perciben las NaaS, cuáles son sus puntos fuertes y limitaciones, y si planean adoptar el modelo de consumo de red emergente.

Esperamos que los datos, las perspectivas y las orientaciones de este informe le ayuden a comprender mejor los beneficios y complicaciones de NaaS a medida que evolucionan sus estrategias de red.

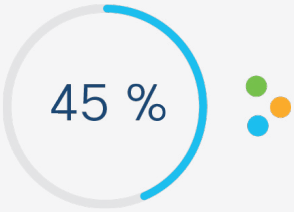
– James Mobley, vicepresidente principal de servicios de redes, Cisco

Descubrimientos clave

No es una propuesta trivial transformar por completo la forma de consumir y operar la red. Necesita un buen negocio y razones tecnológicas para llevar a cabo esta transición a un modelo como servicio. Y necesita partners fiables en quienes confiar para mantener a flote su organización. Aun así, muchas organizaciones están motivadas para pasar a la acción. Estos son algunos descubrimientos clave de nuestra investigación sobre NaaS para 2022:

Descubrimiento clave número 1: desafíos

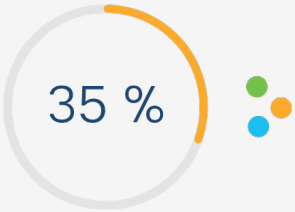
Si la resiliencia y la agilidad son el problema, para muchos, la NaaS es la respuesta.



- La respuesta a las interrupciones (45 %) y la adaptación a nuevas necesidades comerciales (40 %) se citan como los principales desafíos de las redes para 2021.
- Al mismo tiempo, los equipos de TI reconocen los principales beneficios de la NaaS como liberación de los equipos de TI para ofrecer innovaciones y valores de negocios (46 %). Otro 40 % reconoce la NaaS como mejora de la respuesta a las interrupciones y un 34 % como mejora de la agilidad de la red.

Descubrimiento clave número 2: beneficios

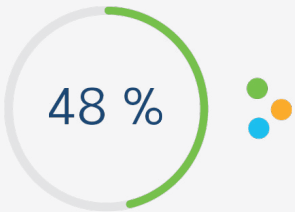
Grandes expectativas: el acceso rápido a las últimas tecnologías es el gran premio.



- La tecnología evoluciona más rápido de lo que las organizaciones pueden adoptar. El 35 % de los encuestados reconoce el requisito de implementación continua de las últimas tecnologías de red, como Wi-Fi 6, la WAN definida por software (SD-WAN), el perímetro de servicio de acceso seguro (SASE), 5G, la inteligencia artificial y otras, como el principal impulsor de las NaaS.

Descubrimiento clave número 3: operaciones

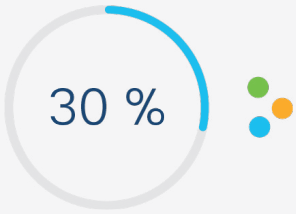
La NaaS es grandiosa, pero solo si ayuda al equipo de redes a cumplir con los acuerdos de nivel de servicio (SLA).



- Los principales servicios requeridos por los proveedores de NaaS son la administración del ciclo de vida de la red (48 %), la recuperabilidad de la red (42 %), y la supervisión y solución de problemas para cumplir con los SLA (38 %).

Descubrimiento clave número 4: problemas

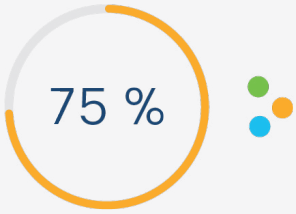
No todo es tan simple; existen inquietudes sobre renunciar al control y los costos.



- Los problemas van desde si la NaaS puede admitir las demandas emergentes que pasan desapercibidas (30 %) hasta la pérdida del control de seguridad (26 %).
- El costo y la interrupción de la transición también tienen una posición elevada (28 %).

Descubrimiento clave número 5: funciones

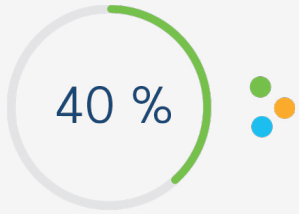
La NaaS abre nuevos horizontes para los profesionales de TI, pero deberán actualizar su labor.



- Más del 75 % de las organizaciones concuerda o concuerda firmemente en que la NaaS brindará a los equipos de TI las oportunidades para desarrollar sus capacidades.
- Sin embargo, en la actualidad, solo 1 de 4 organizaciones confía su propio personal de TI a integradores de sistemas, proveedores de servicios administrados o proveedores de NaaS para traducir sus necesidades comerciales en políticas técnicas.

Descubrimiento clave número 6: adopción

Hay muchas formas de comenzar con la NaaS y una es el SASE.



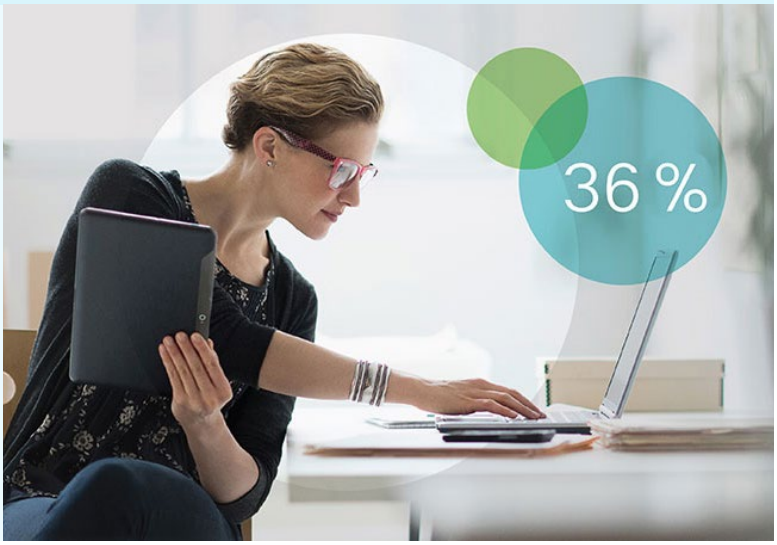
- El SASE es un probable punto de entrada a la NaaS, ya que el 40 % de las organizaciones cita el acceso a la multinube y el 34 % la seguridad como los más adecuados para la NaaS.
- El 49 % de las organizaciones planifica comenzar con la NaaS durante el ciclo de actualización y el 34 % dijo que comenzaría adaptando el sitio existente.

Un modelo de redes diferente

Tras 18 meses de interrupciones y adaptación, la función que desempeñan las tecnologías de red en la supervivencia y el éxito de las empresas nunca ha sido tan clara o esencial. Activadoras clave del trabajo remoto, las redes ahora deben respaldar lugares de trabajo seguro, modelos laborales híbridos y operaciones comerciales en constante evolución. Para ello, deben trabajar sin inconvenientes en todos los entornos del perímetro, la multinube y las instalaciones. Deben brindar una experiencia segura y consistente a todos los usuarios, independientemente de la ubicación, los dispositivos o el método de conectividad. Y deben respaldar tanto las aplicaciones impulsadas por microservicios como las tradicionales.

Dado que los recursos y el ancho de banda a menudo son limitados, muchos líderes de redes y TI están investigando las NaaS como alternativa para abordar estos desafíos. ¿Pero de qué se trata exactamente?

Cuando les pedimos a los líderes de TI una definición de la NaaS, rápidamente pudimos notar que significa algo diferente para cada persona. De hecho, en nuestra encuesta, un sorprendente 36 % de los encuestados afirmó ya contar con NaaS. Si bien parece una cifra alta para una tecnología incipiente, desde las entrevistas pudimos observar que muchos consideran que tienen NaaS cuando parte de la red es administrada por un proveedor externo. Creemos que esta definición es demasiado amplia y necesita más detalles.



La NaaS es un modelo de consumo habilitado en la nube y basado en el uso que permite que los usuarios adquieran y organicen las capacidades de la red sin ser propietarios, sin desarrollar y sin mantener una infraestructura propia.

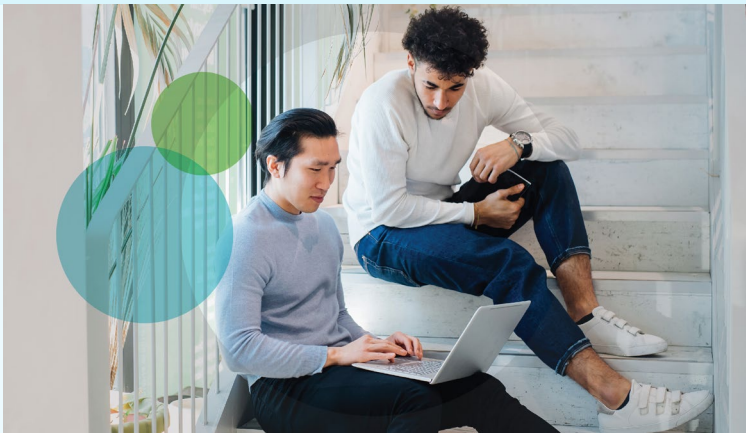
"Las organizaciones intentan determinar la combinación justa de recursos internos y provistos por socios. Muchas eligen invertir en personal, análisis, observabilidad y automatización; piensan arduamente cómo aprovechar a los proveedores estratégicos para liberar la administración de la infraestructura y y el mantenimiento".

– Mary Turner, vicepresidenta de investigación, IDC

La NaaS puede proporcionar un modelo de consumo alternativo para un amplio rango de elementos de red, entre ellos, VPN, WAN y LAN cableadas e inalámbricas, sucursales, centros de datos, perímetros, multinubes y entornos de nube híbridos. Se puede usar para ofrecer nuevos modelos de redes, como el SASE. Puede habilitar cambios en los modelos organizacionales, por ejemplo, el traslado al trabajo híbrido. Como servicio a pedido, la NaaS permite que los equipos de TI escalen hacia arriba o hacia abajo, implementen nuevos servicios rápidamente y optimicen el equilibrio entre CapEx y OpEx.

Para algunos líderes de TI con quienes hablamos, la NaaS representa una nueva y mejor forma de red muy necesaria.

Reconocen que están quedando rezagados y están perdiendo la confianza de sus usuarios. Creen que la NaaS puede ayudarlos a adquirir las últimas tecnologías, cumplir con el creciente conjunto de requisitos y adaptarse al ritmo acelerado de los negocios.



"Con el nivel tan alto de complejidad de la red, la velocidad que deben manejar las empresas para responder a los cambios del mercado y el amplio alcance de las redes modernas, muchas personas se dan cuenta de que 'no pueden seguir haciendo lo mismo y necesitan ayuda'".

— Mark Leary, director de investigación, Análisis de Redes, IDC

Conclusión:

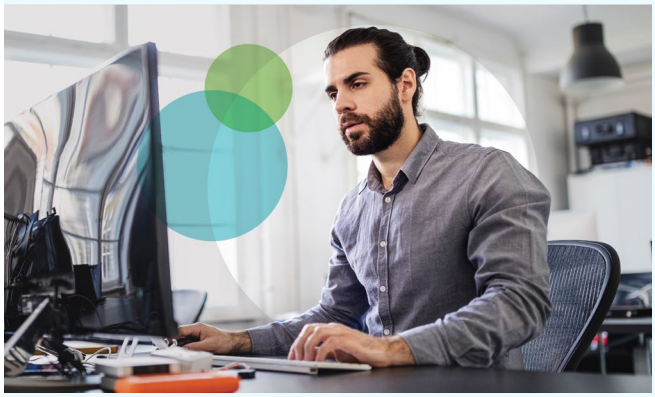
Se espera que la adopción de la NaaS tenga una tasa de crecimiento compuesto anual del 40,7 % de 2021 a 2027.[1]

Abordaje de los desafíos y obtención de beneficios

Elegir la adopción del modelo de NaaS se reduce en última instancia a los desafíos comerciales y tecnológicos que se abordan y los beneficios que se obtienen.

Enelcaso de las organizaciones que encuestamos, la agilidad sigue siendo una prioridad. Cuando les consultamos acerca de los mayores desafíos comerciales que sus redes deben afrontar, casi el 50 % de los profesionales de TI mencionó la respuesta a las interrupciones y el 40 % indicó la adaptación a nuevas aplicaciones comerciales y proyectos empresariales. Más de un tercio de los encuestados identificó la necesidad de agilizar la red como uno de los principales impulsores de la NaaS y la mitad dijo que se anticipan a la NaaS para poder ofrecer mayores innovaciones y valores de negocios.

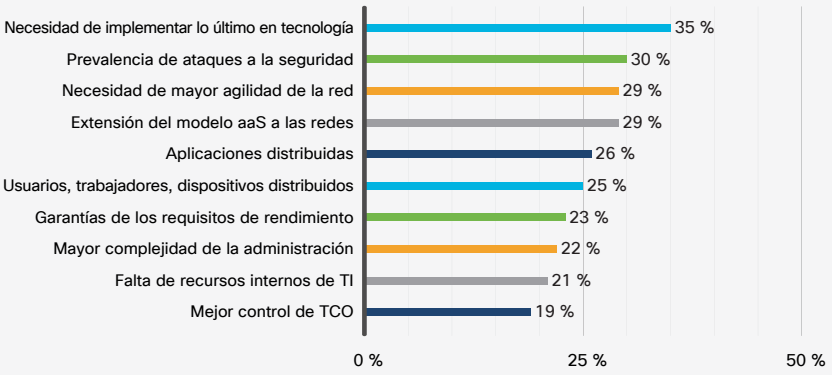
Como parte del esfuerzo para ser más ágiles, muchas organizaciones de TI están pasando sus aplicaciones y servicios a la nube, lo que presenta nuevos retos de seguridad, gestión y cumplimiento.



Según los profesionales de TI que encuestamos, los mayores desafíos tecnológicos que afrontan al administrar las redes en la actualidad son la conexión a múltiples nubes (36 %); la protección de la red, los usuarios y las aplicaciones (34 %); la identificación de causas raíces, y la rápida corrección de la seguridad o los problemas de rendimiento (31 %).

Al mismo tiempo, un tercio de los encuestados identificó la necesidad de implementar continuamente las últimas tecnologías de redes (Wi-Fi 6, SD-WAN, SASE, 5G, IA, etc.) como motivación clave para pasar a la NaaS y otro tercio citó la capacidad de protegerse contra las amenazas a la seguridad, que cada vez son más frecuentes y sofisticadas.

¿Qué haría que traslade su organización al modelo de NaaS?



> "Nuestros ejecutivos no ven valor en el personal que configura los dispositivos u opera la infraestructura. Quieren que TI piense en términos de objetivos comerciales. El uso de servicios externos para las operaciones básicas permite que el personal se acerque a los objetivos comerciales".
>
> — Director de infraestructura de TI, empresa de productos de consumo global

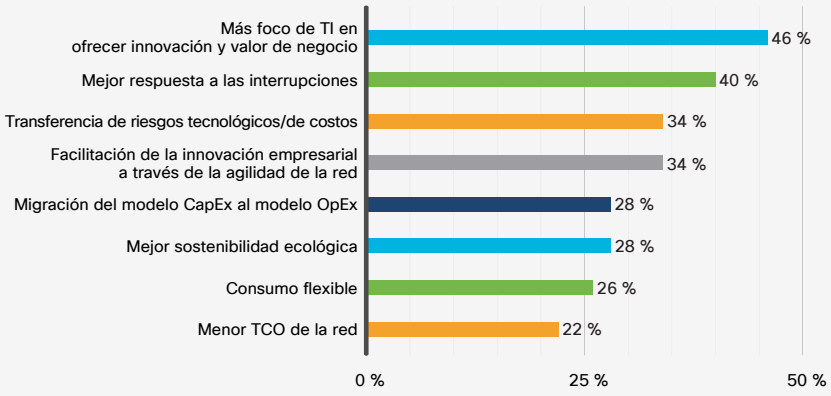
Cuando preguntamos por los principales beneficios que los profesionales de TI esperan de la NaaS, los principales responsables de las decisiones indicaron la capacidad para centrarse en la entrega de valores de negocios en lugar de la administración diaria de la infraestructura.

Mejorar la respuesta a las interrupciones de seguridad y la red fue otro beneficio altamente considerado de la NaaS, como señalaron el 45 % de los profesionales de redes y el 40 % de los principales responsables de las decisiones. Si bien la priorización de las mejoras en seguridad no fue una sorpresa, nos interesó saber que más del 25 % de los profesionales de redes y el 33 % de los principales responsables de las decisiones identificaron la sostenibilidad ecológica mejorada como un gran beneficio de la NaaS.

Aún más sorprendente fue la baja clasificación de los beneficios financieros de la NaaS.

Con un modelo de consumo flexible y precios basados en la suscripción, la NaaS permite que los equipos de TI pasen de gastos de CapEx a OpEx y eviten las grandes inversiones recurrentes en la infraestructura de red. En cambio, los gastos se tornan más consistentes y predecibles y las empresas pagan solo por los recursos que usan. Aun así, estos beneficios fiscales fueron clasificados mucho más abajo por los líderes de TI y los profesionales de redes en comparación con la agilidad, la innovación y los beneficios de liberación de la administración de la NaaS.

En su opinión, ¿cuáles son los principales 3 beneficios comerciales que pueden derivarse del uso del modelo de la NaaS?



Conclusión:

El TCO tiene una baja clasificación en la lista de prioridades cuando se trata de las NaaS porque las empresas están más preocupadas por la entrega de valores de negocios y la respuesta rápida a las interrupciones. El 68 % de los líderes de TI concuerda o concuerda firmemente en que la NaaS liberará a los equipos de la administración diaria de las redes, lo que permitirá más tiempo para centrarse en la entrega de innovación y valores de negocios.

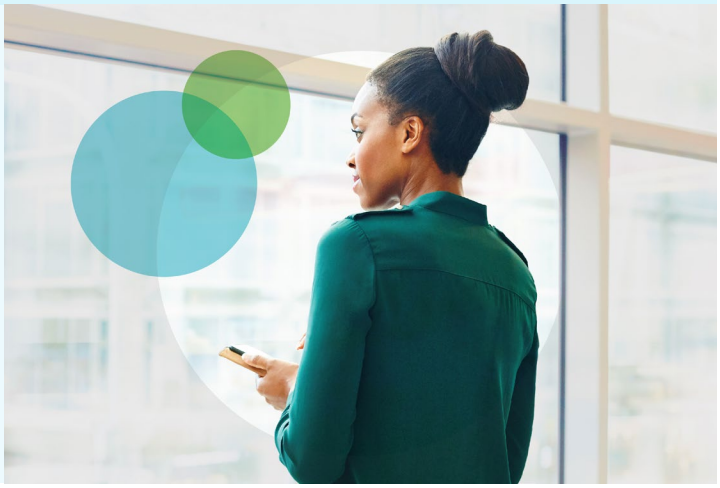
Cómo la NaaS cambia las operaciones de la red (NetOps)

Una inquietud común que hemos escuchado respecto de la NaaS es que requiere un traspaso completo de las operaciones de la red, entregando todas las responsabilidades al proveedor de la NaaS sin dejar nada para el equipo de NetOps de la organización, pero en realidad la NaaS no es un todo o nada cuando se trata de la responsabilidad operativa.

En el modelo de la NaaS, el proveedor asume la responsabilidad de todos los aspectos de la administración del ciclo de vida de la red. Esto incluye la implementación, la integración, el control, la actualización, la supervisión y la reparación de todos los elementos de la infraestructura de la red, incluido cualquier equipo en las instalaciones del cliente, que deban entregar los resultados contractuales. Los resultados pueden incluir la cantidad de usuarios conectados, los sitios, los proveedores en la nube y las aplicaciones, así como los niveles de servicio acordados, el ancho de banda, el rendimiento de las aplicaciones, las provisiones de seguridad, el cumplimiento y otros requisitos.

¿Qué queda para administrar? El equipo de NetOps del cliente de la NaaS podrá centrar más tiempo en actividades principales o de valor agregado.

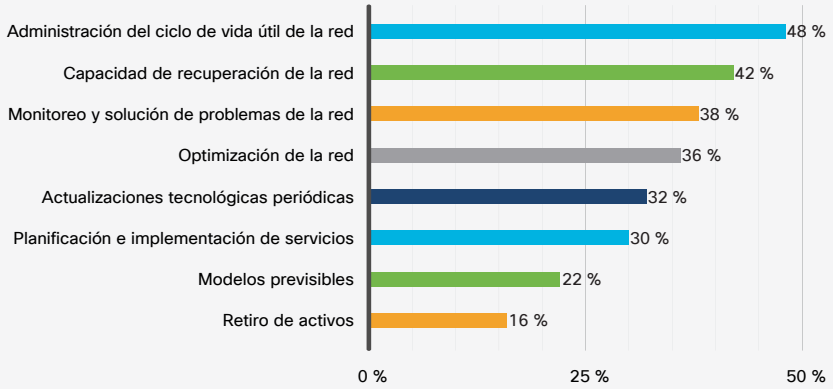
Estas pueden incluir, por ejemplo, la definición y la supervisión de los resultados de la red deseados, como las políticas de acceso a la aplicación y los usuarios y los niveles de rendimiento de las aplicaciones. Al supervisar el rendimiento de la red y los conocimientos, el equipo de NetOps del cliente puede adaptarse continuamente y optimizar las políticas de red y los comportamientos en todos los dominios.



Mediante API, el equipo de NetOps del cliente también puede administrar las integraciones entre la NaaS y los sistemas existentes para optimizar los procesos y flujos de trabajo de TI. Y querrán trabajar junto con el proveedor de NaaS para garantizar que se cumplan los SLA y objetivos a nivel del servicio (SLO). Independientemente de las responsabilidades operativas y las transferencias, queda claro que los profesionales de TI buscan reducir las cargas de la administración de infraestructura.

El 48 % de los profesionales de TI encuestados dijo que la administración del ciclo de vida de la red es el servicio más importante que se debe incluir en el modelo de la NaaS. La recuperabilidad de la red (42 %) y la supervisión y la solución de problemas (38 %) completaron los tres primeros puestos. Esto refuerza la noción de que la administración y la combinación de ubicaciones, usuarios, dispositivos, aplicaciones y recursos de la nube cada vez más distribuidos y complejos deja muy poco tiempo para la innovación y las actividades de valor agregado.

En su opinión, ¿cuál de los siguientes servicios es más importante para incluir en el modelo de la NaaS?



"El proveedor administra las minucias diarias. El equipo interno puede centrarse en la adición de valor a la red abordando los nuevos requisitos a medida que surgen. Nuestros ingenieros y técnicos no tienen que detenerse para solucionar los problemas. Pueden centrarse en nuevos proyectos".

– Ingeniero de redes sénior, empresa de consultoría mundial

Conclusión:

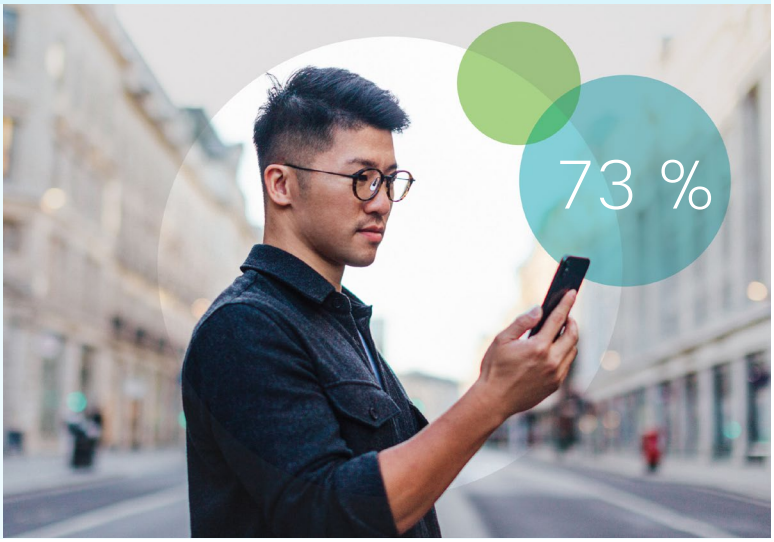
Las responsabilidades operativas se comparten en el modelo de la NaaS. La carga de la administración del ciclo de vida de la red pasa al proveedor, lo que permite que el equipo de TI del cliente se centre más en las actividades operativas que contribuyen al valor del negocio.

Funciones, responsabilidades y capacidades

Al traspasar las responsabilidades de la administración del ciclo de vida de la red y el mantenimiento de la infraestructura al proveedor, la NaaS libera una cantidad de tiempo considerable. Esto permite que el equipo de NetOps del cliente se centre en los resultados deseados de la red en lugar de los aspectos operativos y tecnológicos del mantenimiento de la infraestructura.

En otras palabras, los ingenieros de la red pasan de “pilotar el avión” a “dar las órdenes desde la torre de control”. ¿Pero qué tipo de órdenes se pueden anticipar?

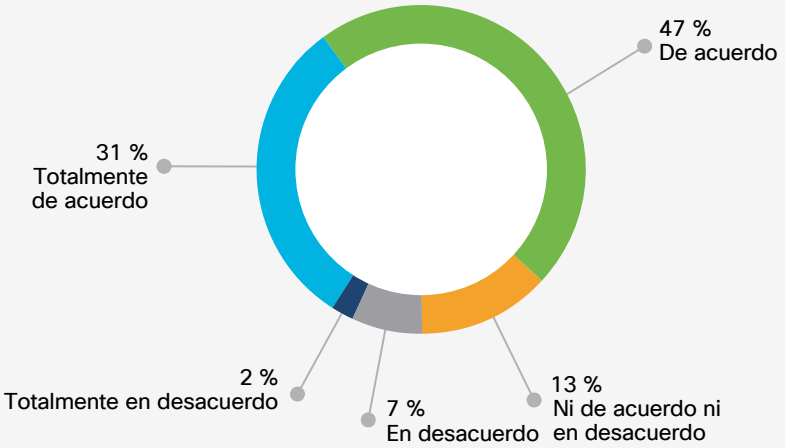
Conforme a los encuestados, el 27 % cree que el personal de TI aprovechará su experiencia técnica y el panel de la NaaS para convertir las necesidades comerciales en políticas de red. Un sorprendente 73 % de los encuestados dijo que prefiere que los proveedores de terceros desempeñen esta función crucial para el negocio, posiblemente indicando una escasez percibida o una falta de confianza en las capacidades internas.

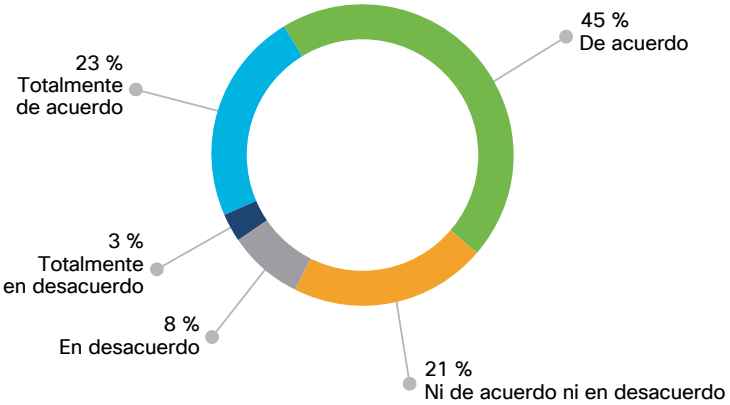


"Con la mayor parte del trabajo diario que pasa al proveedor de la NaaS, el equipo de NetOps del cliente gravitará hacia las habilidades de seguridad de la red y la red general, así como las capacidades diseñadas que convierten las intenciones comerciales en conceptos de redes de alto nivel. Deberá trabajar en estrecha colaboración con el proveedor de la NaaS para optimizar los diseños de la red, las políticas, el rendimiento y los SLA. Y necesitará sólidas habilidades de ciencia de datos para identificar y organizar estos cambios".

– Joe Clarke, ingeniero distinguido, Cisco

Adoptar un modelo de NaaS proporciona a los miembros del equipo de redes oportunidades para mejorar sus habilidades y ofrecer mayor valor a la organización.





La NaaS liberará al equipo de redes para que se centre en las tareas que permiten la innovación de TI y ofrecen valor de negocio en lugar de la administración diaria de las redes.

Conclusión:

Más del 75 % de las organizaciones concuerda o concuerda firmemente en que los modelos de NaaS brindarán a los equipos la oportunidad de desarrollar sus capacidades y ofrecer más valor.

Problemas y dudas

La NaaS afecta muchas áreas de la organización de TI, lo que requiere nuevos modelos de operación, nuevas integraciones con tecnologías y procesos existentes, cambios de funciones y capacidades, y traspaso financiero de CapEx a OpEx. Con estas vastas consecuencias en mente, los profesionales de TI con los que hablamos tienen reacciones diversas ante la NaaS. La mayoría se encuentra en los extremos opuestos del espectro, ya sea muy lejos o muy cerca de la adopción de la NaaS.

Las perspectivas de los líderes de TI respecto de la NaaS parecen reflejar las filosofías de red predominantes. Y esas filosofías primariamente se dividen en dos campos: "TI controlada" y "TI reducida". Los que siguen la primera filosofía no solo tienen un personal altamente calificado, sino también una fuerte creencia en que los equipos deben poseer y controlar por completo la pila de la red. Contrariamente, el último grupo busca consolidar la TI, reevaluar las tareas de rutina frente a las de valor agregado, y buscar formas de liberar el mantenimiento de la infraestructura. No es de extrañar que las organizaciones que piensan en una "TI reducida" que ya han pasado algunos de sus recursos de TI a la nube estén abiertas a las soluciones de NaaS.

> "Estamos demorados con la NaaS porque sentimos que la red no tendrá el cuidado y la priorización que merece y no será el complemento perfecto para nuestro entorno".
>
> – Gerente de TI, redes, agencia militar de los Estados Unidos

Algunos líderes de TI con los que hablamos indicaron que sus redes y procesos son únicos y no consideran que la NaaS pueda abordar sus complejidades y desafíos exclusivos.

Otros expresan una preocupación real respecto de que la NaaS cause turbulencia dentro de la organización de TI.

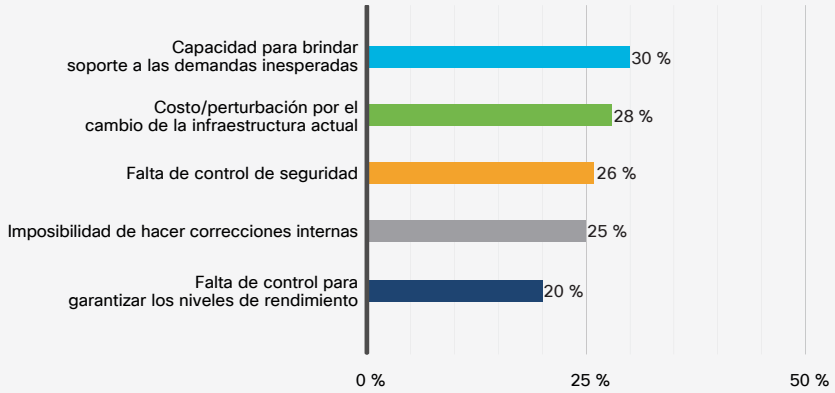
Si bien los líderes de TI comparten un amplio conjunto de inquietudes, predomina la posible pérdida de control entre ellas. El 30 % de los encuestados preguntó si serán capaces de cumplir con las futuras demandas en el caso de que adopten la NaaS. Otros encuestados demostraron preocupación por la pérdida de control de la seguridad (26 %) y el rendimiento (20 %). En la actualidad, la NaaS está diseñada para una mayor escalabilidad a pedido y un soporte más rápido de las tecnologías más recientes. Las decisiones de control sobre seguridad, rendimiento y otras decisiones importantes siguen recayendo en el equipo de TI, no en el proveedor de la NaaS.

"Los proveedores deben adaptarse a nuestras pautas de seguridad y adoptar nuestras directivas. Ese es el principal diferenciador de la NaaS".

— Arquitecto principal, empresa de tecnología global

El 28 % de los encuestados dijo que las interrupciones y los costos asociados con el cambio de la infraestructura existente y las operaciones fueron inhibidores. Comprensiblemente, las organizaciones cuentan con una multitud de tecnologías e inversiones, muchas de las cuales caen en distintos programas de depreciación. Otras organizaciones tienen tecnologías heredadas y aplicaciones que pueden no ser adecuadas para la NaaS. Y otras simplemente no quieren transferir la administración diaria de su infraestructura.

¿Cuáles son sus principales preocupaciones sobre la implementación del modelo de la NaaS?



Para abordar estos problemas y dudas, las organizaciones pueden comenzar de a poco con un dominio para probar nuestro modelo de NaaS. Esto les permitirá comprender mejor las capacidades y los puntos de control de la NaaS sin alterar de manera significativa la infraestructura de red o las operaciones. Podrán experimentar y optimizar la división de responsabilidades entre el proveedor y el equipo interno y aprenderán como trabajar en conjunto para lograr los mejores resultados. Una vez que entiendan por completo y estén cómodas con las funciones, las responsabilidades y los puntos de control, podrán ampliarse y expandirse a otros dominios con el tiempo para aprovechar la información y los procedimientos recomendados aprendidos en el camino.

Conclusión:

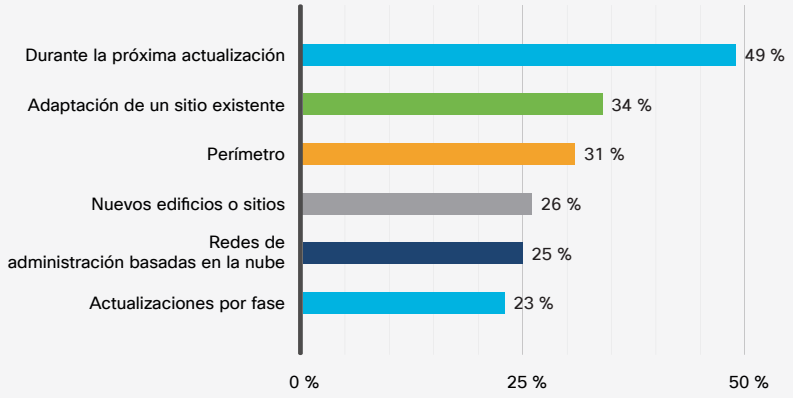
Los problemas son previsibles en cualquier modelo transformacional. Los líderes de TI pueden comenzar de a poco a evaluar los riesgos y las recompensas asociados a la NaaS para ver si es adecuada para la organización.

Tendencias de adopción

Debido al impacto en las operaciones de red y los distintos modos de aprovechamiento, la adopción de la NaaS será diferente para cada organización. Una hoja de ruta de implementación y evaluación de la preparación para la NaaS puede minimizar las complicaciones y maximizar el éxito.

Según los encuestados, el 49 % de los líderes de TI y el 57 % de los profesionales de redes creen que el mejor momento y la mejor circunstancia para adoptar la NaaS es durante la actualización de la infraestructura de la red, cuando se busca acceso a las nuevas tecnologías (automatización, Ethernet de 100 gigabits, Wi-Fi 6, 5G, SD-WAN, SASE, etc.). El 34 % de los encuestados dijo que adaptar un sitio existente (entorno existente) donde la tecnología de red ya está implementada es la situación ideal para la adopción de la NaaS. Resulta interesante que únicamente el 26 % dijo que un emplazamiento nuevo sería la mejor opción para adoptar la NaaS. Y tan solo el 23 % manifestó un enfoque gradual donde los dominios se actualizan uno por uno con la NaaS como el mejor escenario para la organización.

¿Para cuál de las siguientes situaciones cree que la NaaS será la mejor opción para su organización?



Conclusión:

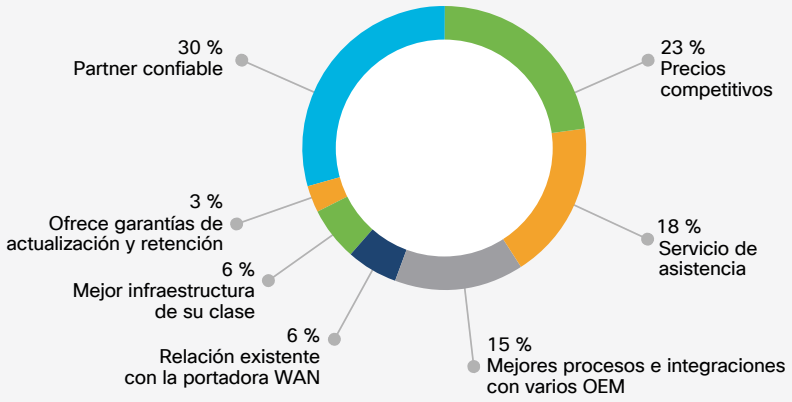
Cómo, cuándo y por qué la implementación de la NaaS será diferente para cada organización.

Elección de un proveedor de NaaS

Dado que la red es un habilitador crucial de la productividad de los empleados, la participación de los clientes y las operaciones comerciales, elegir el proveedor de NaaS correcto no es una tarea trivial. Algunos de los líderes de TI con los que hablamos tienen verdadero temor de perder el control. Y aun así están dispuestos a renunciar a las medidas de control si, y solo si, se ponen en manos de un partner de confianza. Ya sea que esto implique trabajar con un integrador de sistemas, un proveedor de servicios administrados o un reseller de valor agregado, se sienten más cómodos con partners establecidos que tienen conocimiento profundo de su entorno de red, sus objetivos comerciales y sus necesidades de soporte.

Respecto de las implementaciones de la NaaS, casi un tercio de los profesionales de TI en nuestra encuesta considera que los integradores de sistemas son los más confiables y tienen precios más competitivos que los proveedores de redes. Además, mencionó que la “experiencia confiable” es mucho más importante que una “mejor infraestructura”.

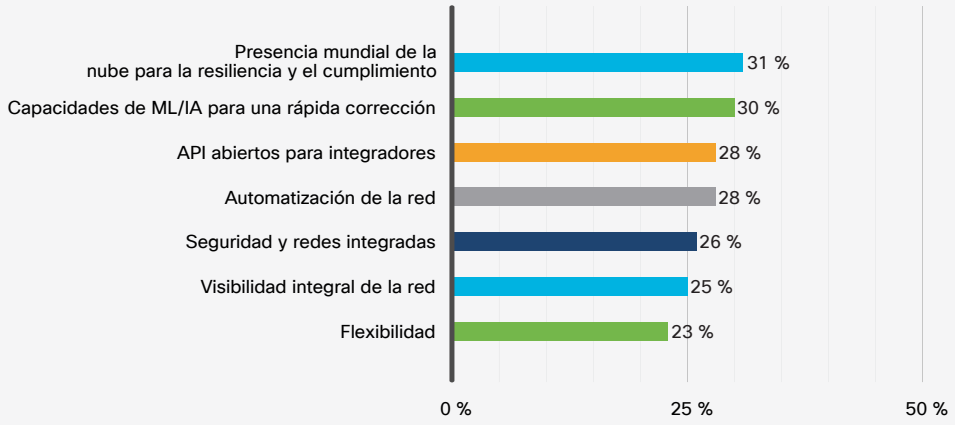
¿Cuál es la razón principal por la que preferiría trabajar con un partner en lugar de trabajar directamente con un proveedor de redes para la implementación de la NaaS?



Cuando se trata de traducir las necesidades comerciales en políticas técnicas, los profesionales de TI son dos o tres veces más propensos a confiar en un integrador de sistemas o en el personal interno de TI antes que en el proveedor de NaaS. Esto se pone de manifiesto en el hecho de que las organizaciones no solo buscan una solución cuando se trata de la NaaS, sino pautas y asistencia de asesores de confianza que las conozcan bien.

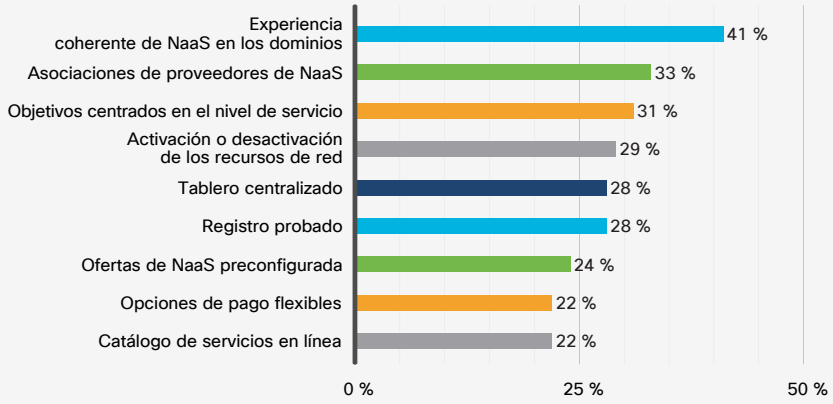
Al considerar los atributos técnicos de las soluciones y los proveedores de NaaS, los encuestados priorizaron la presencia global en la nube para la confianza, el rendimiento y el cumplimiento regional (31 %), así como el aprendizaje automático (ML) y las capacidades de la inteligencia artificial que permiten la optimización continua del servicio de NaaS (30 %). Las API, la automatización, la seguridad integrada, la visibilidad y la flexibilidad de la red también tuvieron una alta clasificación.

¿Cuáles cree que son los 2 atributos técnicos más importantes de la oferta de la NaaS?



El 41 % de los encuestados dijo que es importante que el proveedor de la NaaS ofrezca una plataforma de NaaS consistente en todos los dominios de la red (acceso, WAN, centro de datos, nube, etc.). Con tantos equipos de TI que se esfuerzan por administrar múltiples entornos, conjuntos de herramientas y modelos operativos, la NaaS brinda la oportunidad de consolidar las operaciones, las políticas y los recursos de la red.

¿Cuál de las siguientes opciones es más importante tener al momento de considerar la oferta del proveedor de la NaaS?



"Lo que realmente busco es alguien que pueda manejar las actividades de administración de rutina en la red y los sistemas, como las actualizaciones de firmware, las configuraciones y los cambios. Luego, mi equipo podrá centrarse en las mejoras, el desarrollo y las implementaciones de estrategias. Y tal vez se flexibilice. Tal vez este mes me haga cargo del trabajo pesado y, luego, busque ayuda por un par de meses para expandir el uso y contribuir al trabajo".

– Vicepresidente de tecnología y seguridad, USD 100 millones sin fines de lucro

Conclusión:

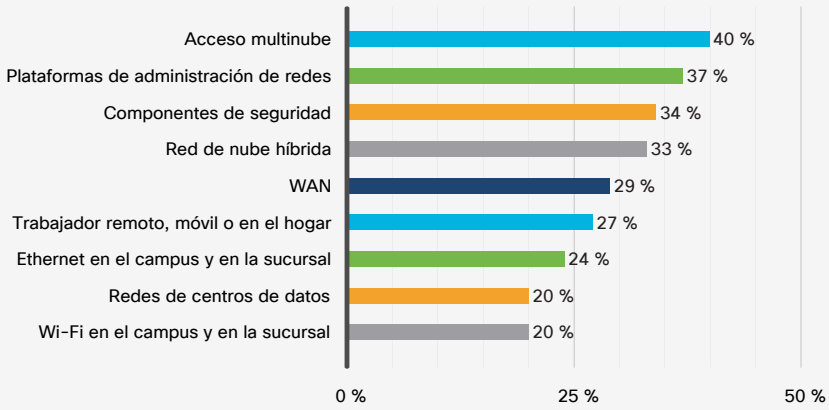
Los integradores de sistemas se consideran más confiables, tienen precios más competitivos y servicios orientados en comparación con los proveedores de NaaS. Independientemente de los proveedores, los clientes buscan experiencia operativa y servicios que expandan todos los dominios de la red.

El SASE y los diferentes tipos de NaaS

Hay una creciente cantidad de ofertas de NaaS, incluidas VPN, WAN y LAN cableadas e inalámbricas, seguridad de la red, acceso remoto o trabajo desde el hogar, redes de centros de datos y redes de nubes. Según nuestra investigación, los modelos de NaaS que incluyen acceso a la multinube y seguridad son los más deseados. Esto quiere decir que SASE, que proporciona acceso a la multinube desde cualquier lugar, es una de las ofertas a pedido como servicio en muchas organizaciones de TI.

Considerando los desafíos de conexión a múltiples nubes dispares, no es sorprendente que se identificara el acceso a la multinube como principal prioridad (40 %) para la NaaS. Al ofrecer servicios de SD-WAN, los proveedores de NaaS pueden ofrecer una forma optimizada y consistente de conectarse a una variedad de aplicaciones basadas en la nube (IaaS y SaaS).

¿Qué aspectos del equipo de la red y la administración son adecuados para la NaaS?

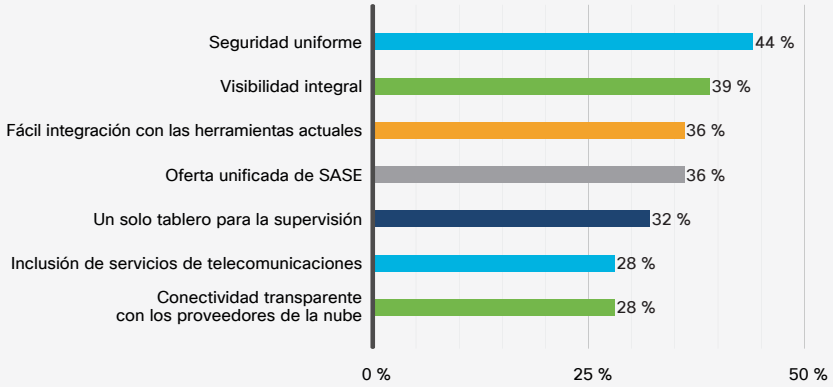


El 34 % de los encuestados priorizó las soluciones de la NaaS centradas en la seguridad, incluidas VPN, administración de eventos e información de seguridad (SIEM), puerta de enlace web segura, firewalls y servicios de prevención y detección de intrusiones (IPS/IDS). Esto puede ayudar a proteger a los usuarios, los dispositivos y las aplicaciones de manera consistente en múltiples nubes y entornos de computación.

Los proveedores de NaaS que ofrecen una combinación de acceso a la multinube y seguridad en el perímetro están bien posicionados para cumplir con la creciente demanda de soluciones de SASE.

Casi la mitad (44 %) de los encuestados citó la “seguridad consistente, incluida la detección y corrección de amenazas, para todos los usuarios y dispositivos”, independientemente desde dónde se accede, como aspecto importante del SASE. Con una creciente confianza en Internet para el acceso a las aplicaciones basadas en la nube, más de uno de tres (39 %) buscan “visibilidad e información sobre el tráfico de red en Internet e infraestructuras en la nube”. Y el 36 % busca soluciones de SASE que se integren fácilmente con las herramientas actuales.

Si su organización debe elegir implementar el SASE como servicio, ¿cuál de las siguientes opciones consideraría como capacidad más importante?



Conclusión:

El acceso a la multinube y la seguridad son las principales prioridades para la NaaS. Los proveedores que entrelazan la opción del SASE con el portafolio de la NaaS pueden cumplir con la creciente demanda para alinear y proteger los recursos en la nube y las instalaciones.

Conclusión

Incontables organizaciones de TI luchan por administrar la complejidad de la red, responder a las interrupciones, proteger a los usuarios y los datos, y seguir el ritmo acelerado de los negocios. A fin de abordar estos desafíos, muchas investigan nuevos modelos de redes, como la NaaS.

LaNaaS ofrece acceso continuo a las últimas tecnologías de redes a través de un modelo basado en suscripción y a pedido. Transfiere la responsabilidad de la administración diaria de redes a un proveedor externo. Al hacerlo, permite que los equipos de TI se centren en las actividades de valor agregado que ofrecen mayor agilidad, recuperabilidad e innovación.

Al igual que cualquier modelo transformacional, existen problemas y dudas en torno a la NaaS. Pero no es una proposición de todo o nada. Los equipos de TI pueden trabajar con partners confiables para probar la NaaS a pequeña escala, evaluar los riesgos y beneficios, y ver si se alinea con sus estrategias integrales de negocio y tecnología.

Asistencia y recursos adicionales

¿Qué es la red como servicio (NaaS)? >

Soluciones Cisco+ >

Encontrar un partner de Cisco >

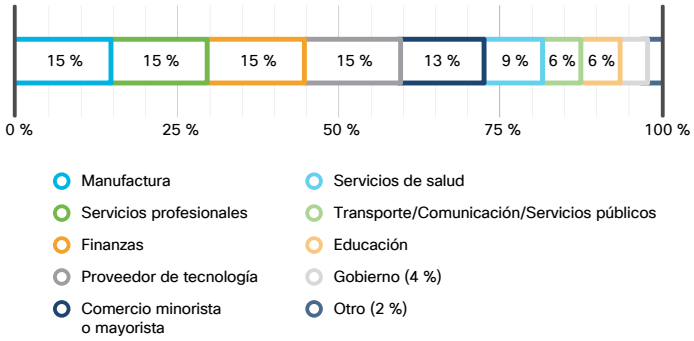
Contacto de ventas de Cisco >

Acerca de este informe

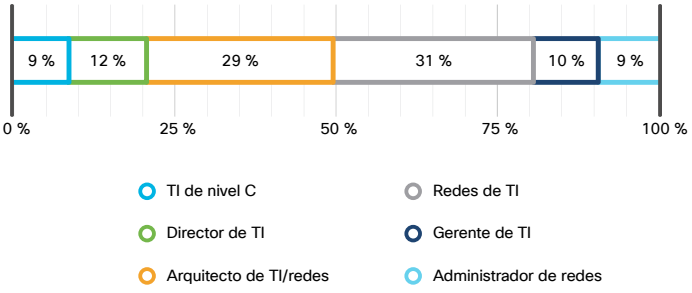
Publicado por primera vez en 2019, el Informe de tendencias globales de redes destaca las últimas estrategias y tecnologías dentro de las redes empresariales y la nube. El informe aprovecha los estudios del sector y ofrece perspectivas, información y orientación para ayudar a las organizaciones de TI a comprender las actuales tendencias tecnológicas, desarrollar sus modelos de redes y respaldar las necesidades comerciales dinámicas.

Para el informe de 2022, realizamos entrevistas con 20 líderes de TI y recibimos la opinión de más de 1534 profesionales de TI en 13 países con respecto a sus perspectivas sobre la NaaS y de qué manera la ven ampliando o alineándose con sus estrategias de red durante los próximos dos años. Los encuestados podían seleccionar hasta tres respuestas por pregunta.

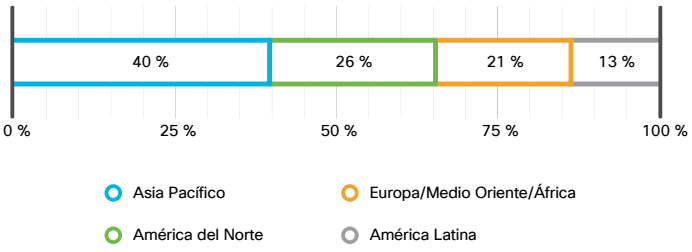
Sector del encuestado



Función del encuestado



Ubicación del encuestado



Permisos para utilizar este informe

Cisco da la bienvenida y anima a la prensa, los analistas, los proveedores de servicios y otras partes interesadas a utilizar la información que contiene este informe. Requerimos el reconocimiento adecuado de todos y cada uno de los datos del informe de tendencias mundiales en redes de 2022 de Cisco que se publiquen o compartan, de forma privada o pública, en formato impreso o electrónico (es decir, “Fuente: informe de tendencias mundiales en redes de 2022, Cisco”). No se requieren más firmas ni consentimientos para referirse a nuestros informes técnicos, informes o herramientas web disponibles públicamente.

Siempre nos interesa el contexto en el que se utilizan nuestros contenidos. Apreciamos que las partes que utilizan nuestro contenido puedan compartir copias de sus trabajos terminados que contengan inserciones del informe de tendencias mundiales en redes de Cisco de 2022. Puede remitir los documentos que contengan referencias sobre el informe de las tendencias mundiales en redes de Cisco de 2022 a networkingtrends-inquiries@cisco.com.

Fuentes de tendencias globales en redes para 2022

1. Dinámicas del sector, tamaño del mercado y pronóstico de oportunidades del mercado global de redes como servicio (NaaS) para 2027, Report Ocean, marzo de 2021.