

Cybersecurity

INSIDERS

2023

Informe de seguridad en la nube



FORTINET®

INTRODUCCIÓN

En 2023, la nube está cumpliendo, fundamentalmente, los resultados de la empresa prometidos, como capacidad y escalabilidad flexibles, mayor agilidad, disponibilidad mejorada e implementación y aprovisionamiento acelerados.

Sin embargo, la preocupación por la seguridad sigue siendo una barrera fundamental para la adopción de la nube, y muestra pocos signos de mejora en la percepción de los profesionales de la seguridad en la nube. La adopción de la nube se ve inhibida además por una serie de desafíos relacionados que impiden una adopción más rápida y amplia de los servicios en la nube, como la continua falta de talento en seguridad en la nube, la proliferación de requisitos de cumplimiento y la significativa falta de visibilidad y control, especialmente en entornos híbridos y de múltiples nubes.

Este Informe de Seguridad en la Nube de 2023 encuestó a 752 profesionales de la ciberseguridad para revelar los principales desafíos y prioridades, incluyendo:

- La seguridad en la nube sigue siendo un problema importante, ya que el 95 % de las organizaciones encuestadas están preocupadas por su postura de seguridad de los entornos en la nube pública. Según el 59 % de los profesionales de la ciberseguridad, la mala configuración sigue siendo el mayor riesgo para la seguridad en la nube. Le siguen de cerca la exfiltración de información confidencial y las interfaces o API no seguras (empatadas a 51 %), y el acceso no autorizado (49 %).
- A pesar de las dificultades económicas, los presupuestos de seguridad en la nube están aumentando para la mayoría de las organizaciones (60 %) en una media del 33 %.
- El 44 % de las organizaciones busca formas de lograr una mejor visibilidad y control en la protección de redes híbridas y de múltiples nubes, y el 90 % busca una plataforma de seguridad única en la nube para proteger los datos de forma coherente y completa en toda su huella en la nube.

Quisiéramos agradecer a [Fortinet](#) por apoyar este importante proyecto de investigación de la industria. Esperamos que encuentre este informe informativo y útil a medida que continúa con sus esfuerzos para proteger la trayectoria a la nube de su organización contra las amenazas en evolución.

Gracias,

Holger Schulze



Holger Schulze

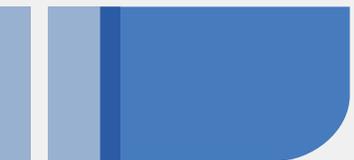
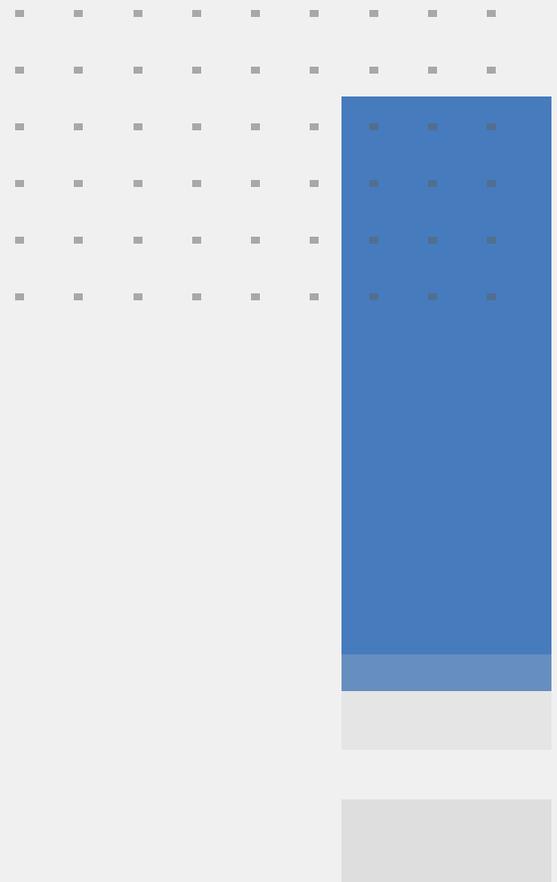
Director ejecutivo y fundador
Cybersecurity Insiders

Cybersecurity
INSIDERS

CONTENIDO

| | |
|---|----|
| ▶ Estado actual de adopción de la nube | 4 |
| ▶ Beneficios de la nube | 10 |
| ▶ Desafíos de seguridad en la nube | 13 |
| ▶ Prioridades clave de seguridad en la nube | 19 |
| ▶ Metodología y demografía | 24 |

Estado actual de adopción de la nube



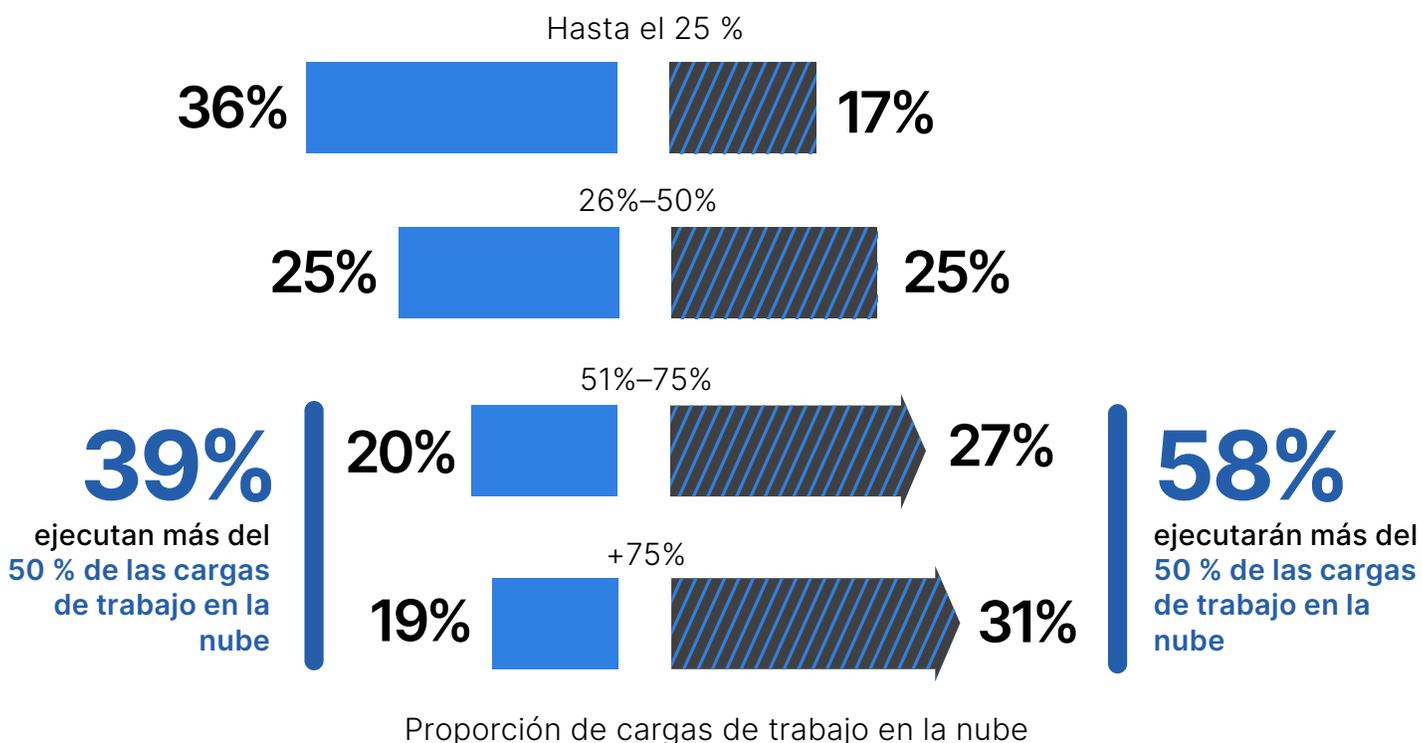
CARGA DE TRABAJO EN LA NUBE

A pesar de la estabilización de la adopción de la nube anual, el ritmo de traslado de cargas de trabajo a la nube sigue siendo fuerte. Actualmente, el 39 % de los encuestados tiene más de la mitad de sus cargas de trabajo en la nube, mientras que el 58 % tiene previsto alcanzar este nivel en los próximos 12 a 18 meses.

▶ Actualmente, ¿qué porcentaje de sus cargas de trabajo está en la nube?

▶ ¿Qué porcentaje de sus cargas de trabajo estará en la nube entre los próximos 12 a 18 meses?

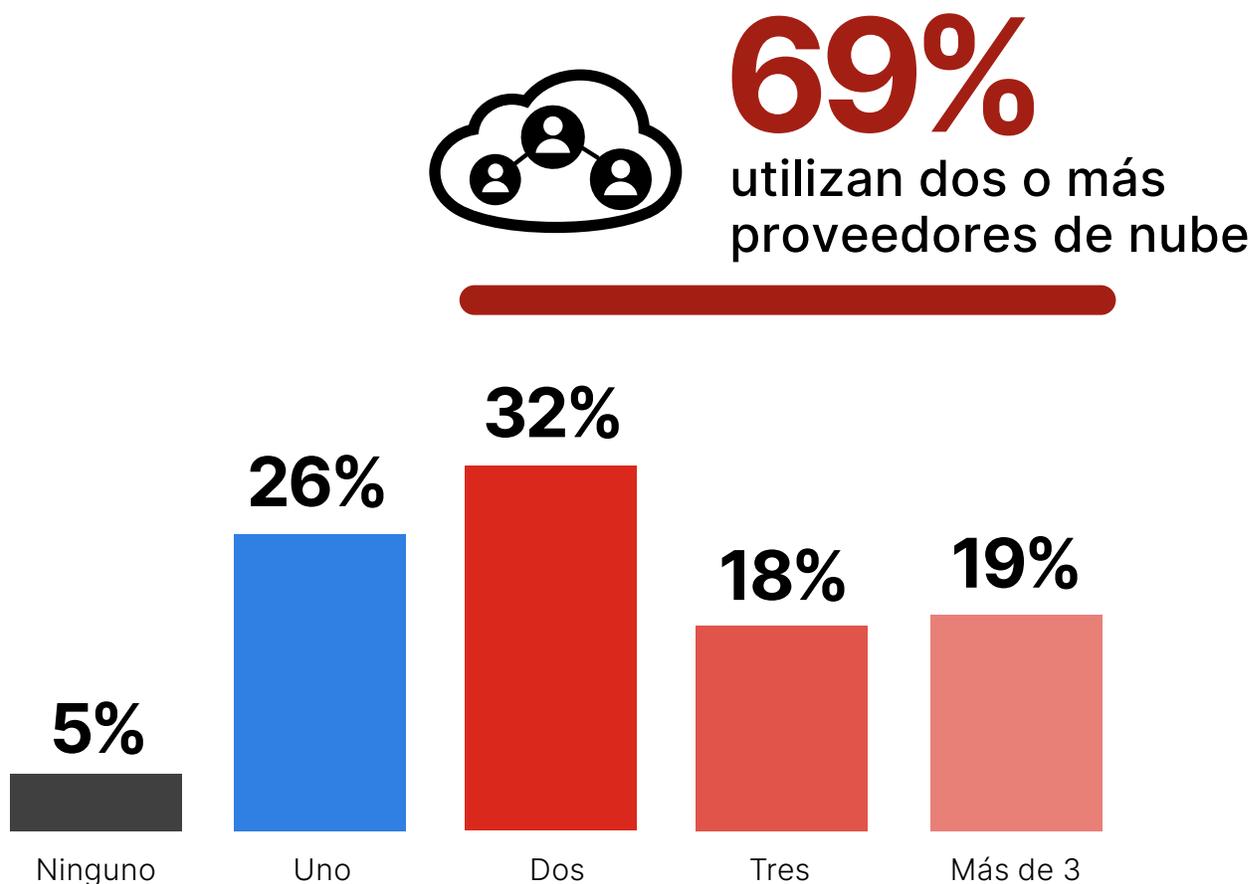
ACTUALMENTE PRÓXIMOS 12 A 18 MESES



ADOPCIÓN DE MÚLTIPLES NUBES

A medida que las cargas de trabajo se trasladan a la nube, las organizaciones seleccionan la plataforma en la nube que mejor se adapta a cada proyecto. Esto está impulsando la proliferación de múltiples nubes, ya que casi siete de cada 10 empresas encuestadas utilizan al menos dos o más proveedores de nube (69 %).

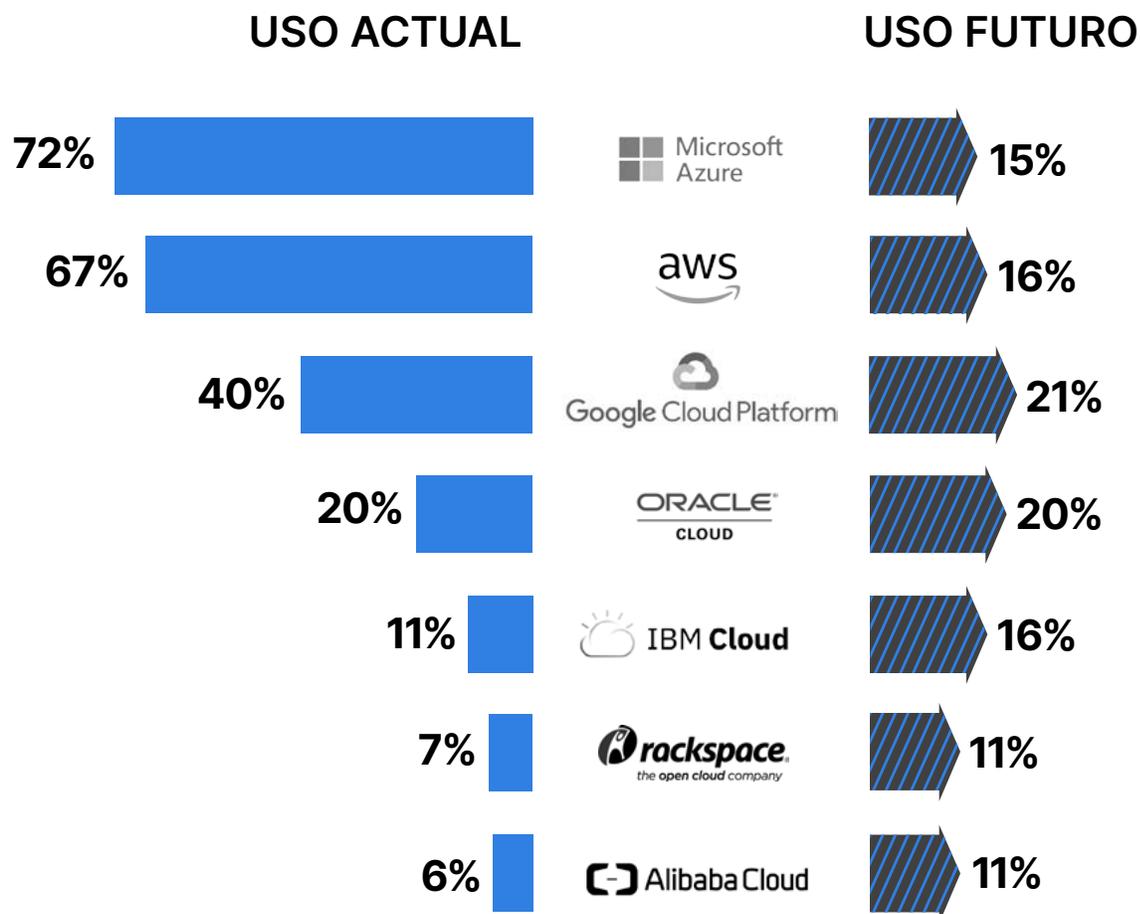
► ¿Cuántos proveedores de nube utiliza actualmente su organización?



PROVEEDORES DE NUBE PREFERIDOS

¿Qué proveedores de nube priorizan las organizaciones? Los grandes proveedores, como Microsoft Azure (72 %) y Amazon Web Services (67 %), siguen dominando el mercado. Sin embargo, la adopción de la nube futura es mayor para Google Cloud Platform (+21 %) y Oracle Cloud (+20 %).

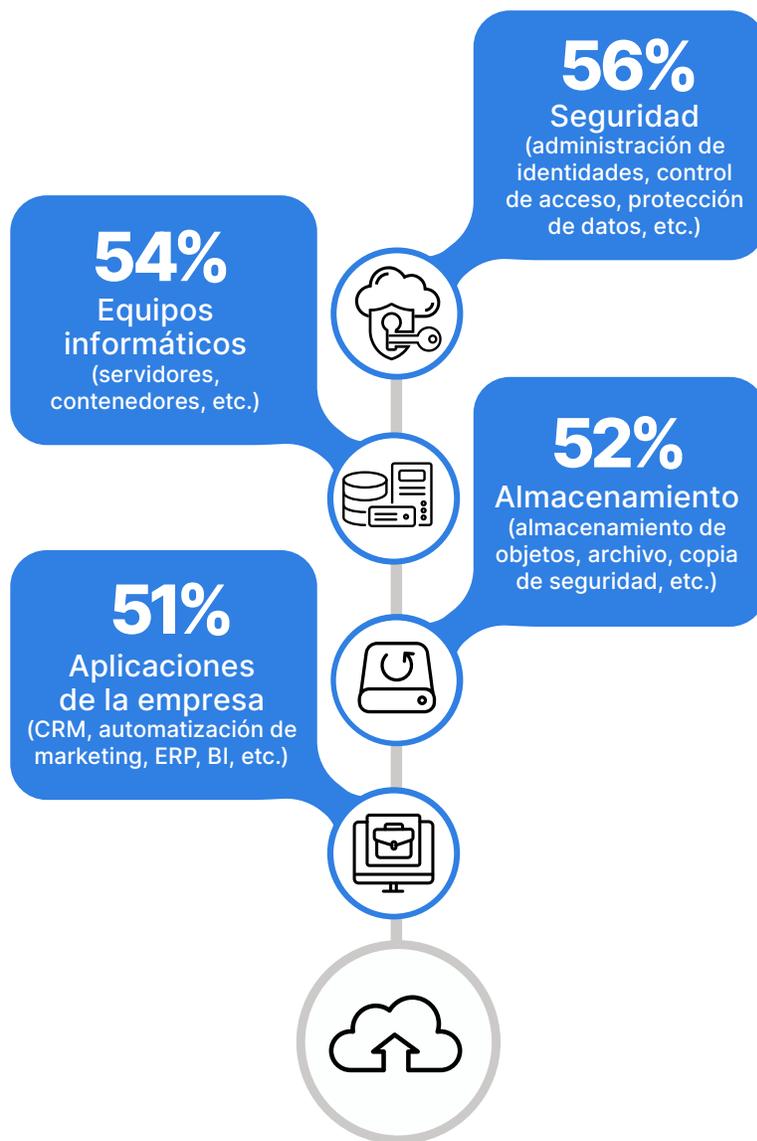
▶ ¿Qué proveedores de IaaS en la nube utiliza actualmente o planea utilizar en el futuro?



PRIORIDADES DE LOS SERVICIOS EN LA NUBE

Parece que la nube no es solo de equipos informáticos y almacenamiento. Curiosamente, los servicios de seguridad son la principal carga de trabajo implementada en la nube (56 %), justo por delante de los equipos informáticos (54 %), el almacenamiento (52 %) e incluso las aplicaciones (51 %).

► ¿Qué servicios y cargas de trabajo está implementando su organización en la nube?



Aplicaciones de productividad (correo electrónico, colaboración, mensajería instantánea, etc.) 50% | Virtualización 49% | Bases de datos (relacional, NoSQL, almacenamiento en caché, etc.) 46% | Aplicaciones de operaciones de TI (administración, copias de seguridad, aprovisionamiento, monitoreo, etc.) 45% | Aplicaciones de desarrollo/pruebas 40% | Redes y entrega de contenidos (nube privada virtual, DNS, etc.) 38% | Sistema operativo 34% | Escritorio y transmisión de aplicaciones 22% | Middleware 22% | Tiempo de ejecución 14% | No sabe/otros 6%

BARRERAS PARA LA ADOPCIÓN DE LA NUBE

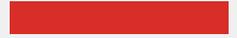
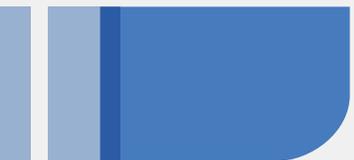
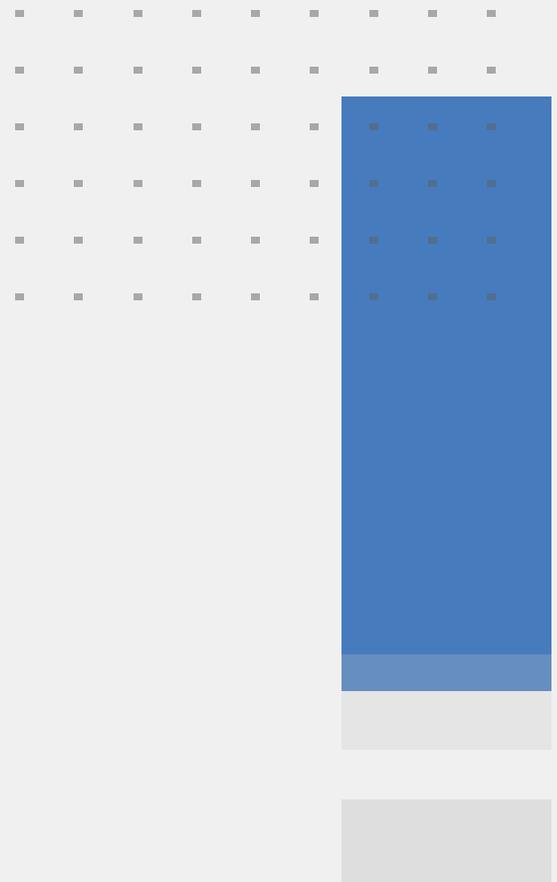
Aunque la nube ofrece importantes ventajas, siguen existiendo barreras significativas para la adopción de la nube. Los mayores desafíos a los que se enfrentan las organizaciones no tienen que ver principalmente con la tecnología, sino con las personas y los procesos. El más crítico es la eterna falta de personal calificado (37 %), que sigue siendo el mayor impedimento para una adopción más rápida, a pesar de haber descendido ligeramente respecto al año pasado. Le siguen de cerca el cumplimiento normativo y legal (30 %), los problemas de seguridad de los datos (29 %) y la integración con el entorno informático existente (27 %).

► ¿Cuáles son las mayores barreras que detienen la adopción de la nube en su organización?



Miedo a la dependencia del proveedor 24 % | Riesgos generales de seguridad 23 % | Falta de presupuesto 22 % | Costo/falta de ROI 21 % | Resistencia interna e inercia 20 % | Pérdida de control 19 % | Complejidad en la administración de la implementación de la nube 18 % | Falta de transparencia y visibilidad 15 % | Problemas de facturación y seguimiento 14 % | Falta de madurez de los modelos de servicios en la nube 13 % | Falta de participación de la gerencia 13 % | Insatisfacción con las ofertas, el rendimiento y los precios de los servicios en la nube 12 % | Falta de personalización 10 % | Falta de soporte por parte del proveedor de la nube 8 % | Rendimiento de las aplicaciones en la nube 8 % | Disponibilidad 8 % | Otros 5 %

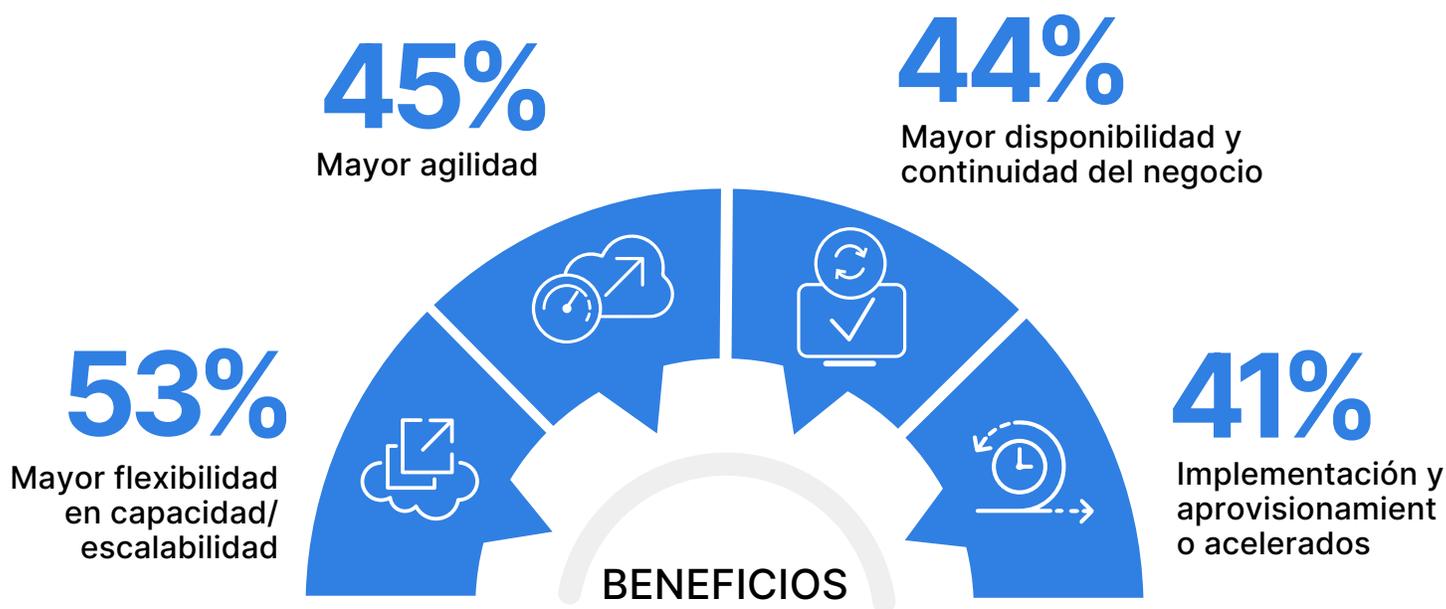
Beneficios de la nube



BENEFICIOS CLAVE DE LA NUBE

Después años de adopción de la nube, ¿creen las organizaciones que la computación en la nube está cumpliendo sus promesas? La respuesta es afirmativa. Los usuarios de la nube afirman que esta ofrece beneficios clave para la empresa, como flexibilidad y escalabilidad (53 %), agilidad (45 %), continuidad del negocio (44 %) e implementación y aprovisionamiento acelerados (41 %). Este es el primer año en el que la implementación acelerada se ha situado entre los cuatro primeros, superando tanto al rendimiento como al cambio a OpEx variable.

► ¿Qué beneficios generales obtuvo ya de su implementación en la nube?

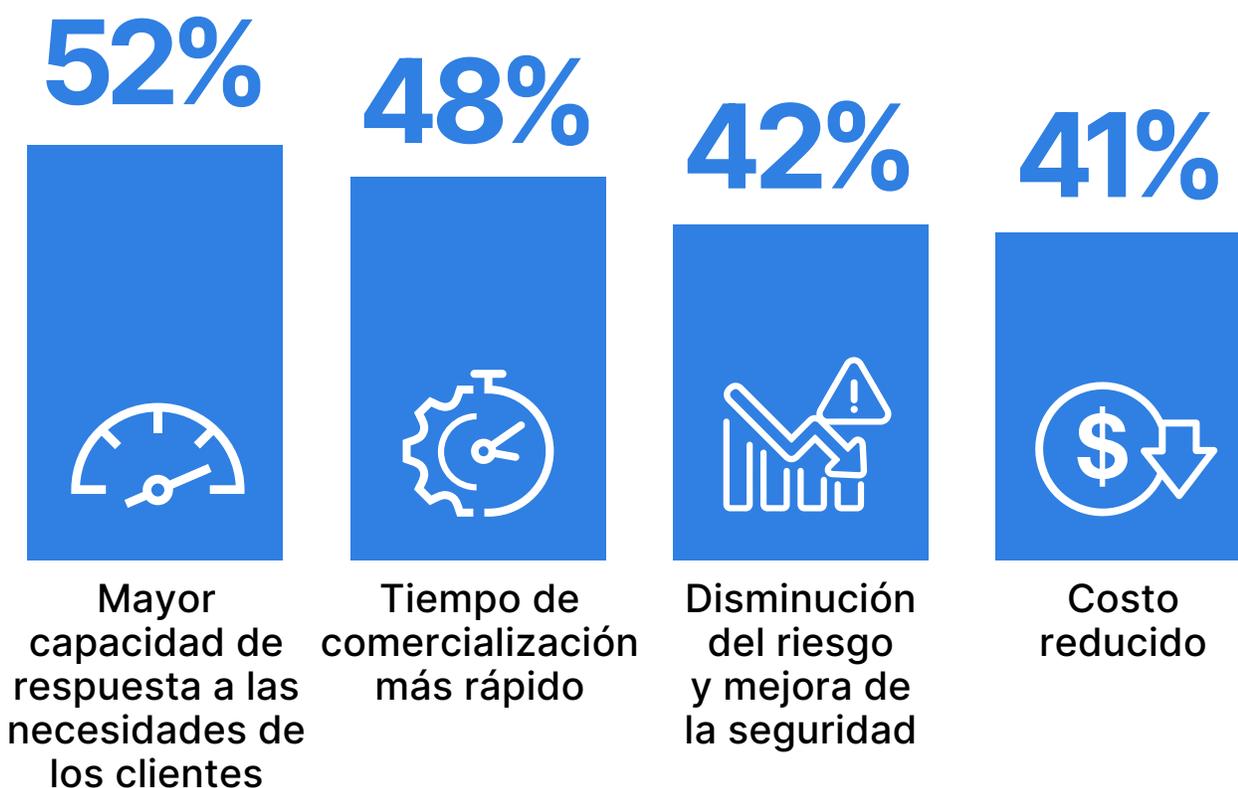


Mejor rendimiento 36 % | Tiempo de comercialización más rápido 34 % | Traslado de gastos de CapEx fijos (compra) a OpEx variables (alquiler/suscripción) 34 % | Costo reducido 32 % | Mejora de la seguridad 32 % | Mayor alcance geográfico 27 % | Aumento de la productividad de los empleados 25 % | Reducción de la complejidad 23 % | Mejor cumplimiento normativo 22 % | No estoy seguro/otros 12 %

RESULTADOS DE LA EMPRESA EN LA NUBE

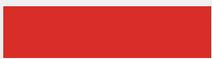
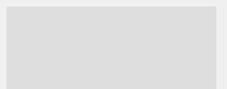
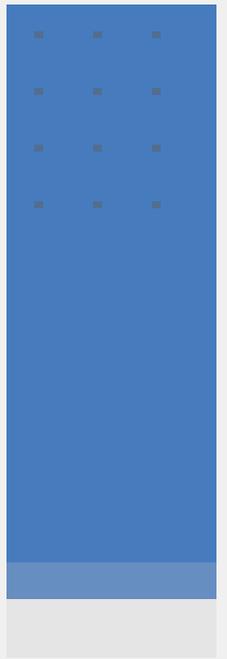
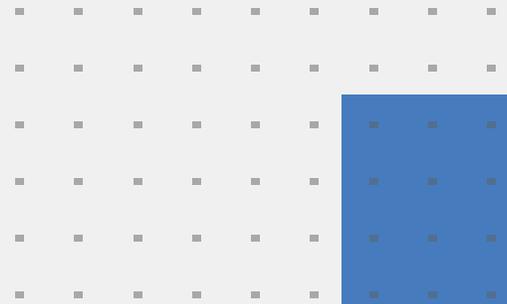
Los beneficios de la nube están impulsando los resultados de la empresa clave, y este año la capacidad de respuesta a las necesidades de los clientes (52 %) se convierte en el principal resultado, en lugar de tiempo de comercialización más rápido (48 %). Las organizaciones que son inteligentes a la hora de integrar la ciberseguridad en su paso a la nube también están viendo su valor para el negocio en un menor riesgo y una mayor seguridad (42 %) y en la reducción de costos (41 %).

► ¿Qué resultados de negocio ha obtenido al pasar a la nube?



Mayor alcance a nuevos mercados 23 % | Aceleración del crecimiento de los ingresos en los mercados existentes 22 % | Paridad con los competidores 22 % | Otros 7 %

Desafíos de seguridad en la nube



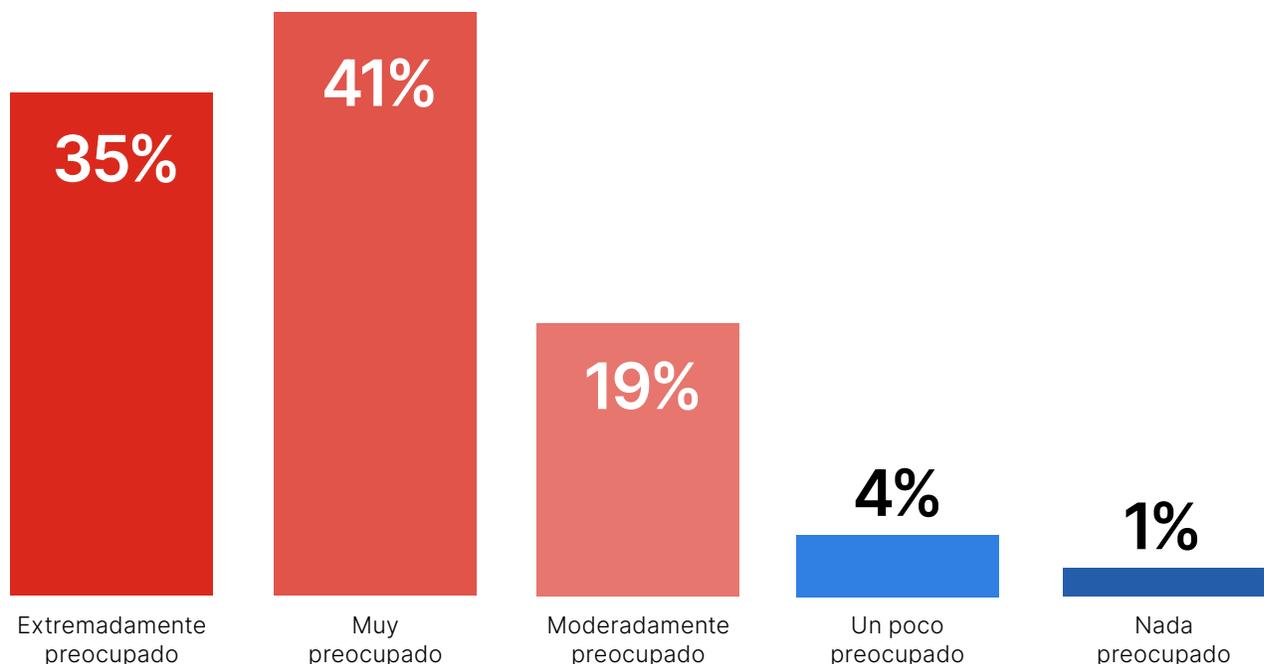
PREOCUPACIONES DE SEGURIDAD EN LA NUBE PÚBLICA

A pesar de la creciente adopción de la nube, la preocupación sobre la seguridad de las nubes no muestra mejorías. Prácticamente todas las organizaciones encuestadas están entre moderada y extremadamente preocupadas por su postura de seguridad en entornos en la nube pública (95%). El número de organizaciones extremadamente preocupadas por la seguridad de la nube pública incluso aumentó este año: un 35%, frente a un 32%.

► ¿En qué medida le preocupa la seguridad en las nubes públicas?

 **95%**

de las organizaciones están moderadamente o extremadamente preocupadas por la seguridad en la nube



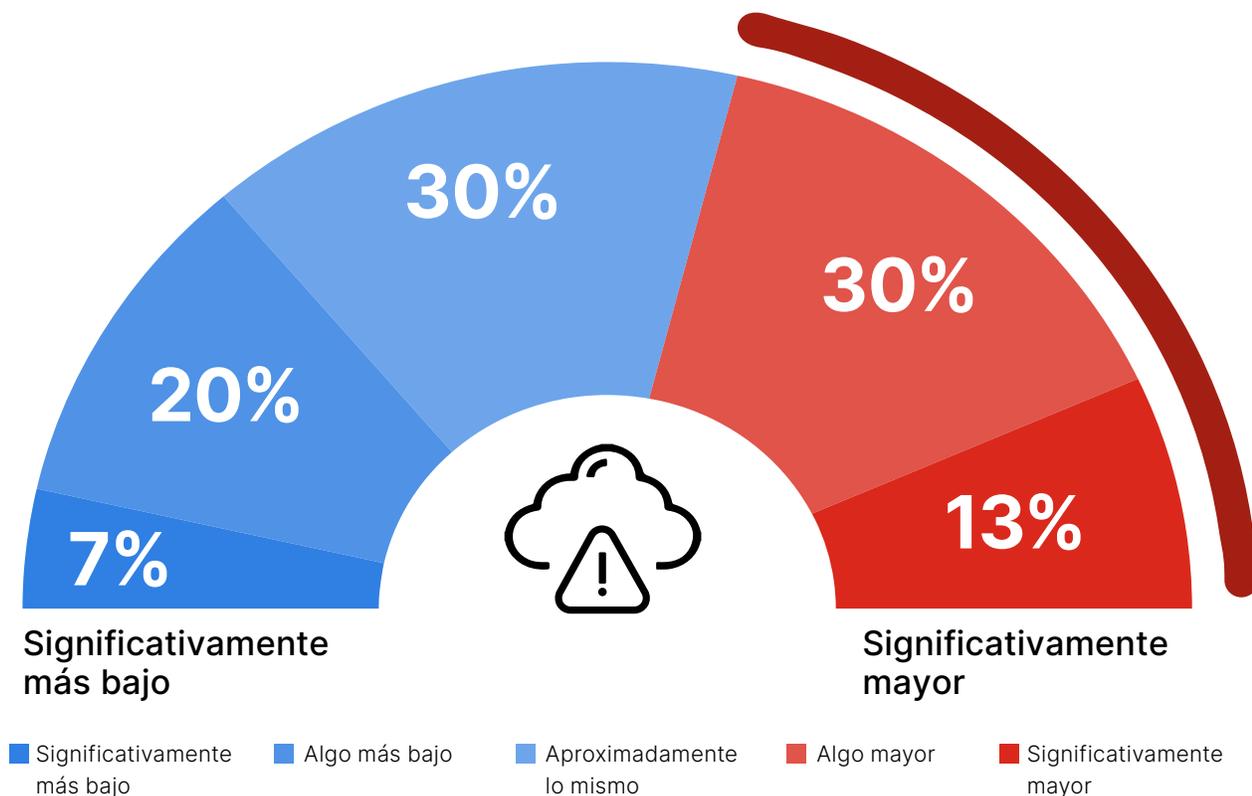
RIESGO DE VIOLACIÓN DE SEGURIDAD

La preocupación por la seguridad en la nube pública, combinada con la falta de recursos y experiencia, está impulsando la percepción de que el riesgo de una violación a la seguridad de la nube pública es mayor que en los entornos tradicionales locales (43 %). Solo el 27 % de los profesionales de la seguridad perciben que el riesgo es menor en un entorno de nube pública.

► En comparación con los entornos de TI tradicionales, ¿diría que el riesgo de violaciones de seguridad en un entorno de nube pública es mayor o menor?

43%

afirman que el riesgo de la nube pública es, algo o significativamente mayor, que el de la nube local



PROBLEMAS DE SEGURIDAD OPERATIVA

Los profesionales de la ciberseguridad se enfrentan a numerosos desafíos al proteger las cargas de trabajo en la nube. El factor humano vuelve a encabezar la lista: la falta de personal de seguridad calificado (43 %), seguido de cerca por el cumplimiento (37 %). La proliferación de múltiples nubes es casi, con toda seguridad, la razón de los problemas que supone la aplicación de políticas de seguridad uniformes (32 %).

► ¿Cuáles son sus mayores problemas de seguridad operativa y cotidianos al proteger las cargas de trabajo en la nube?

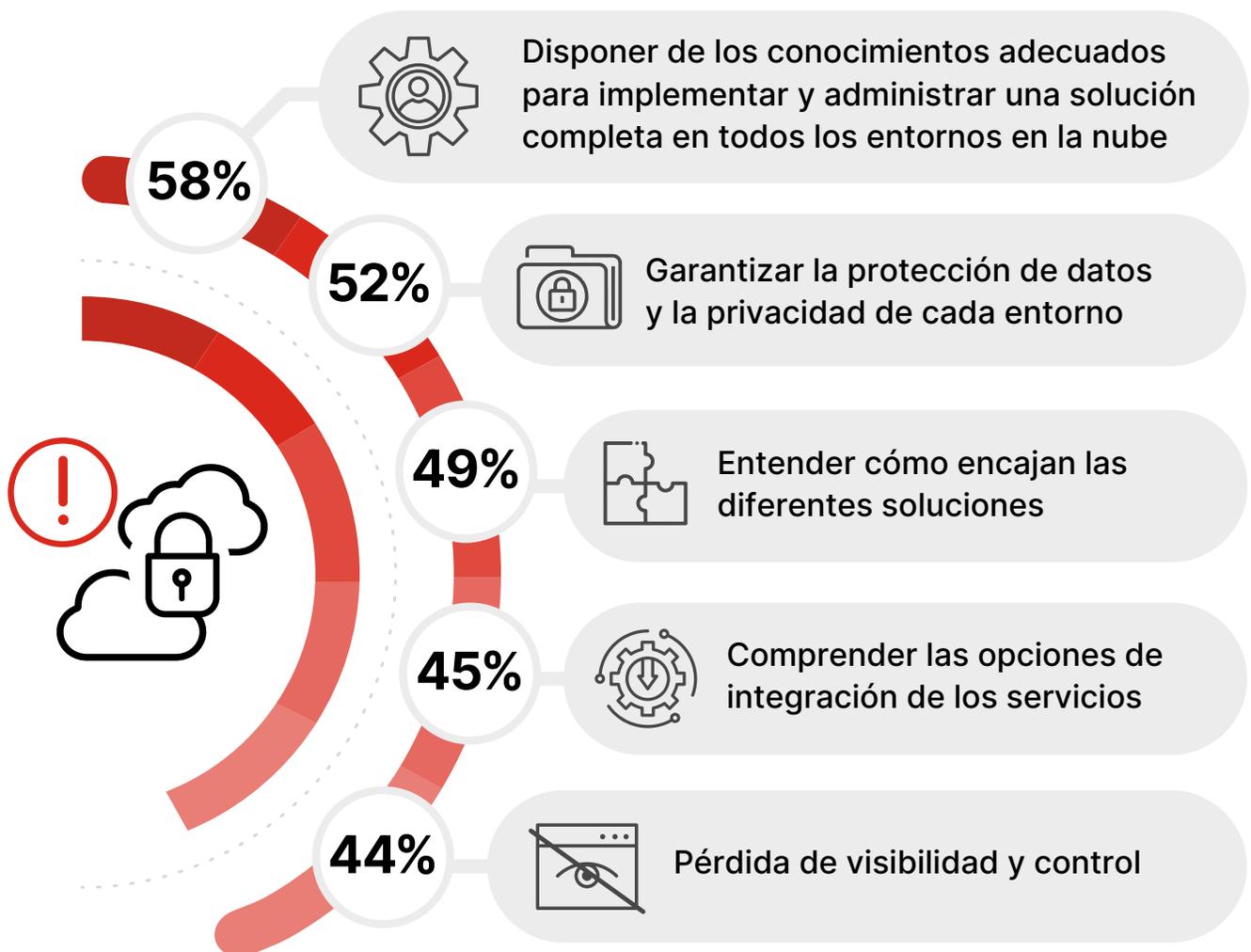


Controles y automatización 30 % | No se pueden identificar rápidamente los errores de configuración 29 % | Aplicación automática de la seguridad en múltiples nubes 29 % | Compleja correspondencia de reglas de seguridad de nube a nube/nube a local 25 % | Protección de los flujos de tráfico 25 % | Protección del acceso desde dispositivos móviles y personales 25 % | La seguridad no puede seguir el ritmo de los cambios en las aplicaciones nuevas/existentes 25 % | Falta de integración con las tecnologías de seguridad locales 25 % | Establecimiento de privilegios de acceso de usuario correctos 24 % | Eliminación de amenazas 24 % | Justificación de un mayor gasto en seguridad 24 % | Comprensión de los patrones de tráfico de la red 23 % | Ausencia de detección/visibilidad/control automático de la seguridad de la infraestructura 22 % | Notificación de amenazas a la seguridad 21 % | Falta de paridad de funciones con la solución de seguridad local 21 % | Falta de flexibilidad 6 % | No estoy seguro/otros 10 %

DESAFÍOS DE LA SEGURIDAD DE MÚLTIPLES NUBES

Los entornos de múltiples nubes aumentan la complejidad y los desafíos de la seguridad de las cargas de trabajo en la nube. El factor humano y los conocimientos que exigen los entornos de múltiples nubes se ponen claramente de manifiesto en el hecho de que tres de los cuatro desafíos principales están relacionados con disponer de las habilidades adecuadas, junto con un conocimiento profundo de cada plataforma en la nube.

► ¿Cuáles son sus mayores desafíos a la hora de asegurar los entornos de múltiples nubes?



Seguir el ritmo de los cambios 38 % | Administrar el costo de las diferentes soluciones 37 % | Proporcionar un acceso fluido a los usuarios en función de sus credenciales 37 % | Seleccionar el conjunto de servicios adecuado 36 % | Otros 3 %

AMENAZAS A LA SEGURIDAD EN LA NUBE

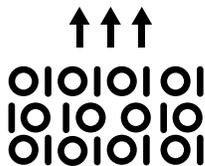
¿Qué amenazas a la seguridad en la nube inquietan a los profesionales de la ciberseguridad? Las mismas cuatro que el año pasado, con la configuración incorrecta en primer lugar, según el 59 % de los profesionales de la ciberseguridad. Le siguen de cerca la exfiltración de información confidencial y las interfaces o API no seguras (empatadas a 51 %) y el acceso no autorizado (49 %).

► ¿Cuáles considera que son las mayores amenazas para la seguridad en las nubes públicas?



59%

Mala configuración de la plataforma en la nube o configuración incorrecta



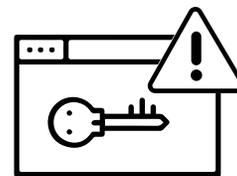
51%

Exfiltración de información confidencial



51%

Interfaces o API no seguras

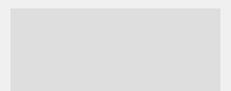
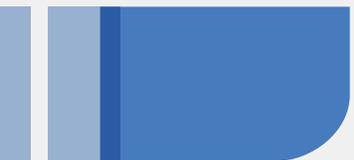
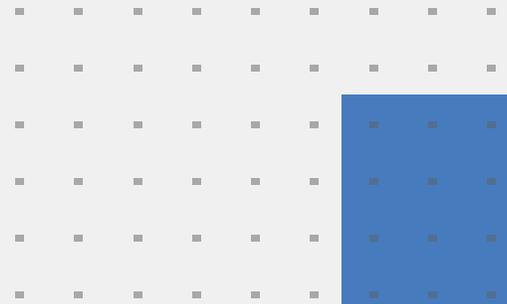


49%

Acceso no autorizado

Secuestro de cuentas, servicios o tráfico 45 % | Intercambio externo de datos 39 % | Personas maliciosas con información privilegiada 38 % | Malware/ransomware 37 % | Ciberataques patrocinados por estados extranjeros 37 % | Ataques de denegación de servicio 31 % | Criptojackening en la nube 21 % | Robo de servicio 20 % | Pérdida de dispositivos móviles 13 % | No sabe/otros 7 %

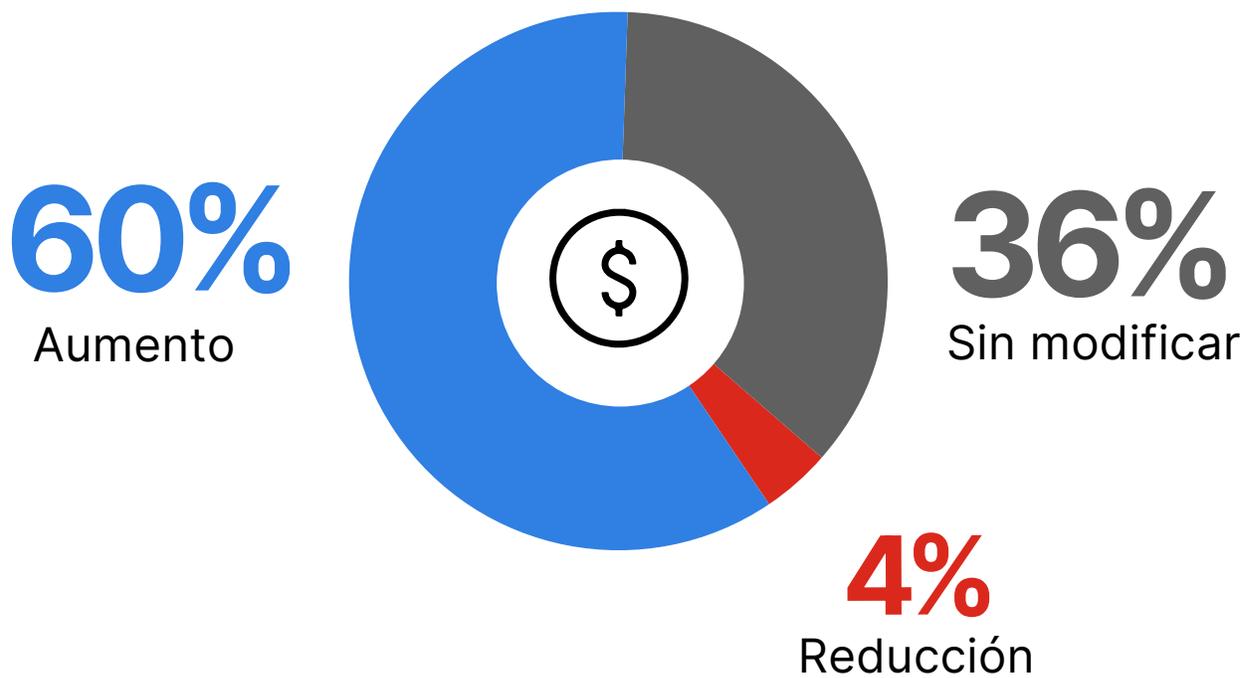
Prioridades clave de seguridad en la nube



PRESUPUESTO DE LA NUBE

A pesar de las dificultades macroeconómicas y de la reducción de las cargas de trabajo que se trasladan a la nube en comparación con años anteriores, la mayoría de las organizaciones (60 %) aumentará su presupuesto de seguridad en la nube este año. Se espera que ese aumento suponga un incremento del 33 % en el poder adquisitivo interanual.

► ¿Cómo cambiará su presupuesto de seguridad en la nube en los próximos 12 meses?



► Si el presupuesto de su programa de seguridad va a aumentar, indique ¿en qué porcentaje?



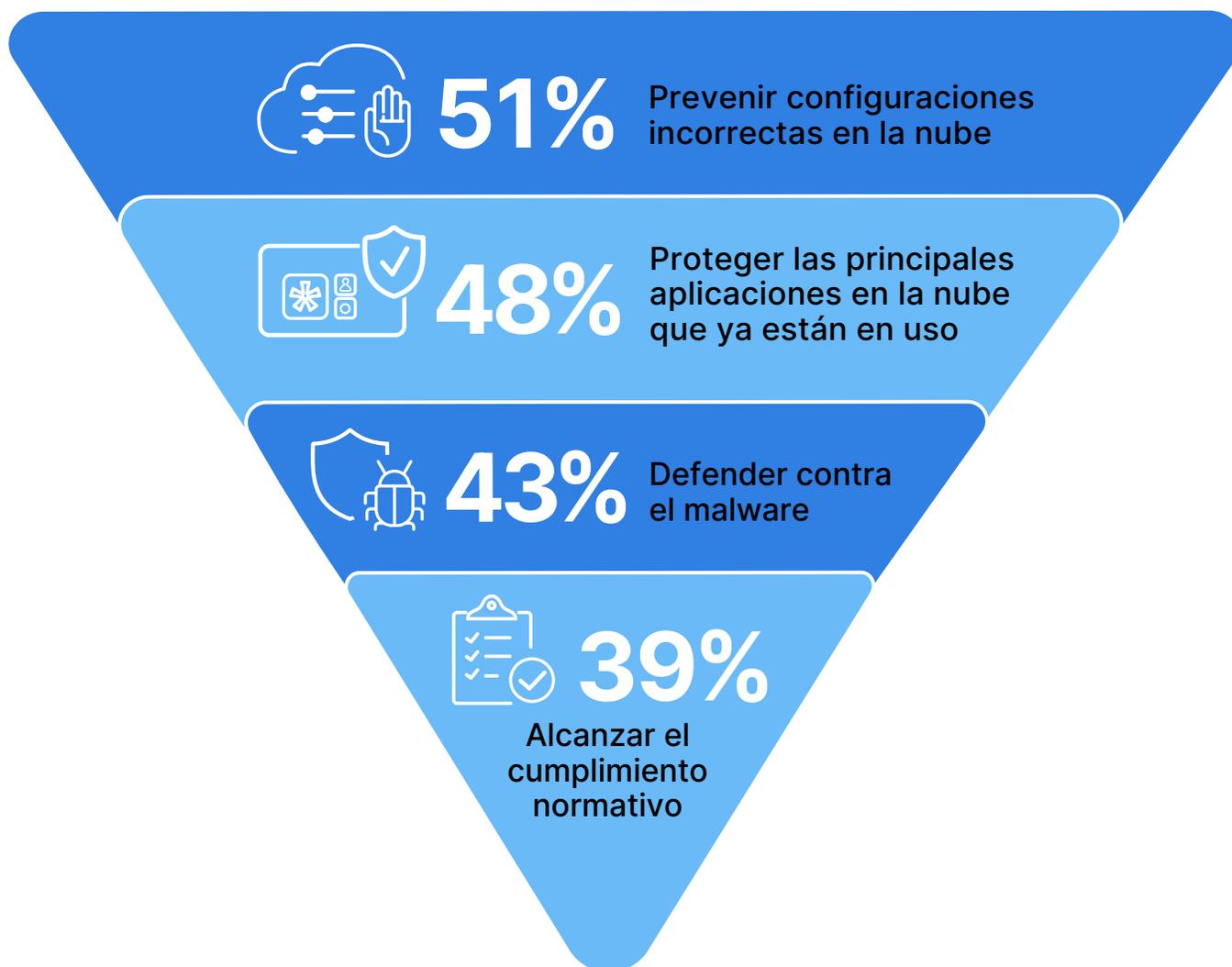
El presupuesto aumentará

33%

PRIORIDADES DE SEGURIDAD EN LA NUBE

Los profesionales de la seguridad están utilizando sabiamente sus presupuestos de la nube para abordar las amenazas y preocupaciones que plantean el mayor riesgo para la empresa. Puede que no sorprenda que la prevención de la configuración incorrecta sea la prioridad (51 %), pero la seguridad de las aplicaciones que ya se trasladaron a la nube ocupa un cercano segundo lugar (48 %).

► ¿Cuáles son las prioridades de seguridad en la nube para su empresa este año?



Capacitación de seguridad en la nube 12 % | Protección de dispositivos móviles 7 % | Descubrimiento de aplicaciones en la nube no autorizadas en uso 7 % | Protección de BYOD (traiga su propio dispositivo) 5 % | Protección de las aplicaciones en la nube menos populares ya en uso 4 %

IMPULSORES CLAVE PARA LA **SEGURIDAD** **BASADA EN LA NUBE**

La nube permite a las organizaciones obtener los mismos beneficios para sus servicios de seguridad que para sus aplicaciones y cargas de trabajo. Esto incluye una mejor escalabilidad (56 %), un tiempo de implementación más corto (48 %), un esfuerzo mínimo con respecto a parches y actualizaciones de software y actualizaciones de software (43 %) y un ahorro de costos (40 %).

▶ ¿Cuáles son los principales impulsores para considerar soluciones de seguridad basadas en la nube?

56%



Mejor
escalabilidad

48%



Tiempo de
implementación
más corto

43%



Esfuerzo mínimo
con respecto
a parches y
actualizaciones
de software

40%



Ahorro de
costos

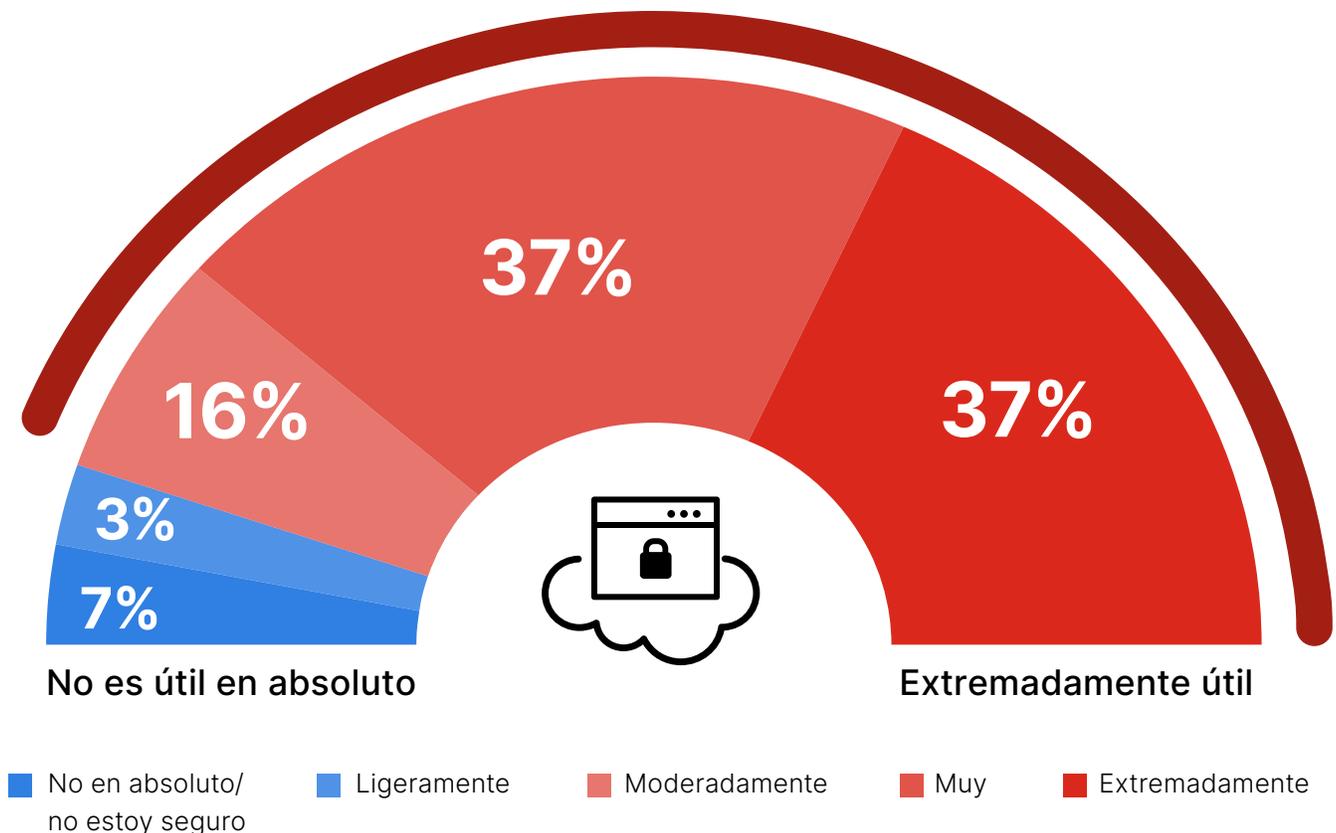
Mejor visibilidad de la actividad del usuario y del comportamiento del sistema 38 % | Mejor tiempo de actividad 36 % | Administración de políticas más simple 35 % | Cubre las expectativas de cumplimiento de la nube 35 % | Mejor rendimiento 35 % | Necesidad de acceso seguro a la aplicación desde cualquier lugar 34 % | Nuestros datos o cargas de trabajo se alojan en la nube (o se están trasladando a la nube) 30 % | Reducción del espacio que ocupa el appliance en las sucursales 29 % | Otros 3 %

PLATAFORMA ÚNICA DE SEGURIDAD EN LA NUBE

A la luz de los desafíos relacionados con la visibilidad de la seguridad y la falta de cibertalentos, no es de extrañar que la gran mayoría de los encuestados (90 %) considere que es de moderada a extremadamente útil tener una plataforma de seguridad única en la nube y de un panel de control para proteger los datos de manera uniforme y completa en todo su espacio en la nube.

▶ ¿Qué tan útil sería tener una sola plataforma de seguridad en la nube con un único panel de control en el que pudiera configurar todas las directivas necesarias para proteger los datos de manera consistente y completa para toda su presencia en la nube?

90% de los profesionales consideran que el uso de una plataforma de seguridad única en la nube con un panel único es moderada o extremadamente útil



METODOLOGÍA Y DEMOGRAFÍA

El Informe de seguridad en la nube de 2023 se basa en una encuesta global integral de 752 profesionales de ciberseguridad que se efectuó en febrero de 2023, para develar cómo las organizaciones de usuarios de la nube están adoptando la nube, cómo ven la evolución de la seguridad en la nube y qué mejores prácticas priorizan los líderes de ciberseguridad de TI en su traslado. Los encuestados incluyen desde ejecutivos técnicos hasta profesionales de seguridad de TI, lo que representa una muestra representativa equilibrada de organizaciones de varios tamaños en múltiples industrias.

NIVEL PROFESIONAL



DEPARTAMENTO



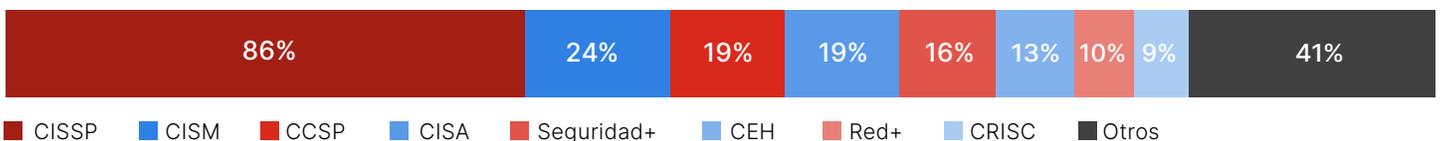
TAMAÑO DE LA EMPRESA



INDUSTRIA



CERTIFICACIONES DE SEGURIDAD OBTENIDAS





Fortinet (NASDAQ: FTNT) protege a las más grandes empresas, proveedores de servicios y organizaciones gubernamentales en todo el mundo. Fortinet brinda a sus clientes un control y visibilidad completos en toda superficie de ataque creciente y la capacidad de asumir los requisitos de rendimiento cada vez mayores, actuales y futuros. Solamente la plataforma del Fortinet Security Fabric puede abordar los desafíos de seguridad más críticos y proteger datos en toda la infraestructura digital, ya sea en entornos de red, de aplicaciones, de múltiples nubes o perimetrales. Fortinet ocupa el primer lugar como la empresa con más appliances de seguridad distribuidos en todo el mundo y más de 635,000 clientes confían en Fortinet para proteger sus empresas.

www.fortinet.com/lat



Cybersecurity

I N S I D E R S

Cybersecurity Insiders es una comunidad en línea de más de 500,000 miembros para profesionales de la seguridad de la información, que reúne a los mejores expertos especializados en promover la ciberseguridad y proteger a las organizaciones en todas las industrias, tamaños de empresas y puestos de seguridad.

Proporcionamos a los profesionales del marketing de ciberseguridad [oportunidades de marketing únicas](#) para llegar a esta audiencia calificada y ofrecer contenido de liderazgo de opinión para la validación de terceros basado en hechos, programas de generación de demanda y visibilidad de marca en el mercado de la ciberseguridad.

**Para obtener más información, visite
www.cybersecurity-insiders.com**