

2024

Informe de Seguridad en la Nube



FORTINET®

Introducción

Las empresas están adoptando cada vez más una estrategia centrada en la nube mediante el desarrollo y la implementación de aplicaciones teniendo en cuenta la nube. Dado que la mayoría de las organizaciones adoptan un enfoque híbrido o de múltiples nubes para admitir diversos casos de uso y modelos de trabajo, la superficie de ataque se ha ampliado significativamente, lo que hace que proteger los entornos de nube actuales sea más crítico y cada vez más complejo.

El Informe de seguridad en la nube 2024, basado en una encuesta exhaustiva de 927 profesionales de la ciberseguridad en todo el mundo, proporciona información crítica sobre las tendencias actuales que impulsan la seguridad en la nube. Explora los desafíos clave en la protección de entornos de nube complejos, qué soluciones y estrategias están priorizando los profesionales de la ciberseguridad, cómo asignan sus recursos y las mejores prácticas que están adoptando para garantizar la seguridad de las cargas de trabajo en la nube.

Los hallazgos clave incluyen:

- **Preferencia de múltiples nubes:** La mayoría de las organizaciones (78 %) optan por estrategias híbridas y de múltiples nubes. para combinar flexibilidad, control y los beneficios únicos de varios servicios en la nube.
- **Barreras de adopción de la nube:** Las preocupaciones de seguridad y cumplimiento (59%) son obstáculos críticos para una adopción más rápida de estrategias de múltiples nubes. Los desafíos técnicos (52%) y las limitaciones de recursos (49%) presentan desafíos sustanciales para lograr visibilidad y control de políticas dentro de infraestructuras complejas de múltiples nubes y enfatizan la necesidad de contar con una sólida experiencia en seguridad en la nube.
- **Escasez de talento en ciberseguridad:** Las empresas enfrentan una escasez crítica de experiencia en ciberseguridad, y el 93% de los encuestados está preocupado por encontrar profesionales calificados para proteger entornos complejos de múltiples nubes. Esto afecta directamente su postura de seguridad y sus esfuerzos estratégicos. Esta persistente escasez de experiencia en seguridad en la nube obstaculiza una adopción más rápida y generalizada de estrategias de múltiples nubes.
- **Preferencia de plataforma unificada de seguridad en la nube:** El 95% de los encuestados abogan por una única plataforma para optimizar la seguridad en todos los entornos de nube. El objetivo es simplificar y automatizar la gestión de la seguridad, mitigar la brecha de talento y mejorar la seguridad mediante la aplicación consistente de políticas y la visibilidad, abordando las ineficiencias de la gestión de múltiples sistemas de seguridad dispares.

Nos gustaría agradecer a [Fortinet](#) por el invaluable apoyo a este importante proyecto de investigación de la industria. Esperamos que este informe sirva como una guía práctica para que los líderes y profesionales de la ciberseguridad naveguen por las complejidades de la seguridad en la nube de manera más efectiva en sus esfuerzos continuos para proteger el viaje a la nube de su organización contra las amenazas cibernéticas en evolución.

Gracias,

Holger Schulze

Founder, Cybersecurity Insiders

Cybersecurity
INSIDERS

Estrategias de Implementación en la Nube

Elegir la estrategia de implementación de la nube adecuada es fundamental para que las organizaciones maximicen los beneficios de la computación en la nube y al mismo tiempo minimicen los riesgos asociados.

La mayoría de las organizaciones (78%) favorecen una estrategia híbrida o de múltiples nubes, integrando múltiples implementaciones en un único entorno operativo. Una gran parte de esto (43%) utiliza un híbrido de nube e infraestructura local. El 35% de las organizaciones tiene una estrategia de múltiples nubes, lo que destaca una preferencia por aprovechar las fortalezas de diferentes proveedores de servicios en la nube para una variedad de casos de uso. Sólo el 22% depende de un único proveedor de nube, lo que sugiere un enfoque centrado que simplifica la gestión pero que puede aumentar la dependencia de un solo proveedor.

► ¿Cuál es la estrategia principal de su organización para la implementación de la nube?



Nube híbrida

43%



Multinube

35%



Nube única

22%

78% de las organizaciones utilizan una nube múltiple o entorno híbrido

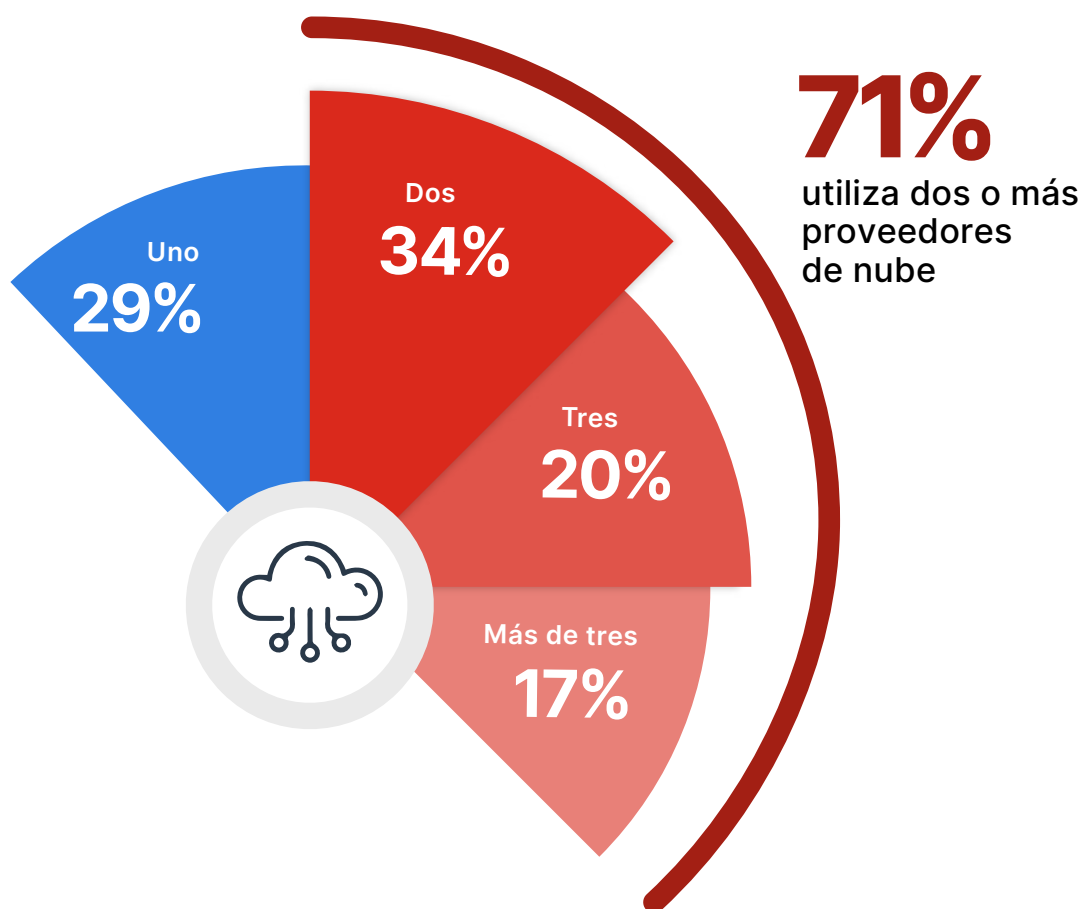
Para navegar mejor las complejidades de las implementaciones híbridas y de múltiples nubes, las organizaciones deben priorizar un marco de seguridad integrado que garantice una protección perfecta en toda su huella digital. Esto es esencial para ofrecer la agilidad, la escala y la seguridad necesarias para una defensa sólida contra las ciberamenazas en evolución.

Adopción de Múltiples Nubes

La cantidad de proveedores de nube que utiliza una organización es crucial, lo que afecta la flexibilidad operativa, la gestión de riesgos y la complejidad de las implementaciones de seguridad. La mayoría de las organizaciones (71%) utilizan dos o más proveedores de servicios en la nube, lo que indica un enfoque que busca combinar flexibilidad, control y los beneficios únicos de cada proveedor de servicios en la nube. Un aumento de 2 puntos porcentuales con respecto a la encuesta del año pasado refleja un cambio creciente hacia estrategias de múltiples nubes, impulsado por la necesidad de servicios de nube especializados, disponibilidad regional y redundancia.

Curiosamente, sólo el 29% de las organizaciones dependen de un solo proveedor de nube, lo que pone de relieve una preferencia por la simplicidad y tal vez una asociación estratégica con un único proveedor de nube.

► ¿Cuántos proveedores de nube utiliza actualmente su organización?



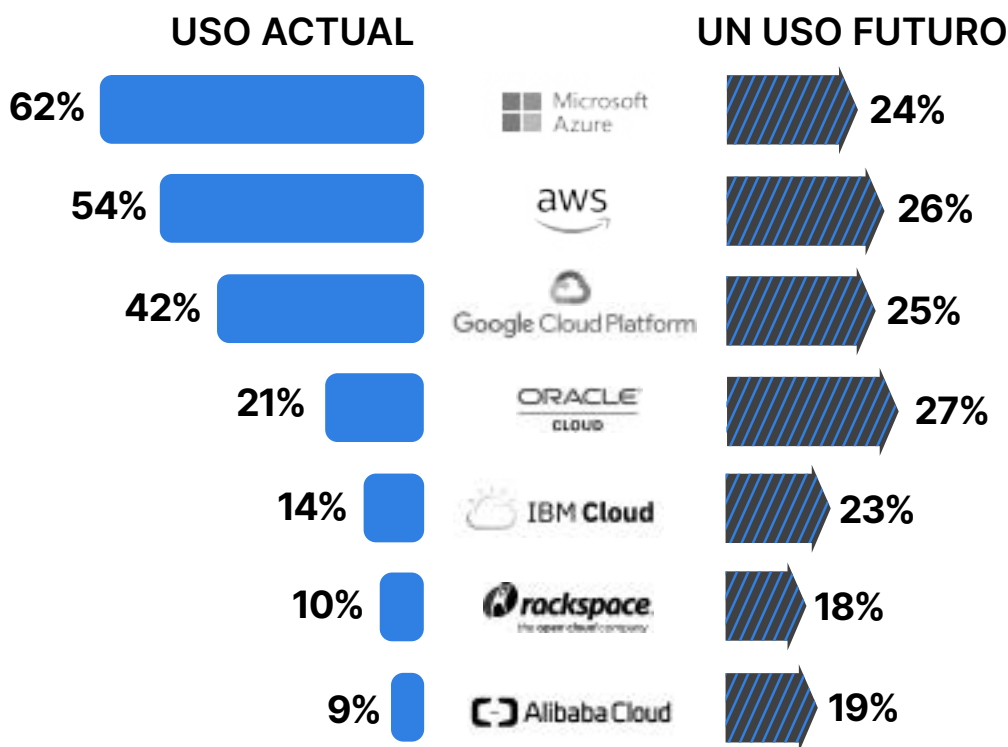
Las organizaciones deben adoptar un enfoque fluido y neutral respecto de la nube para proteger múltiples entornos de nube que garantice políticas de seguridad consistentes y visibilidad en toda su huella digital, reduciendo la complejidad y reforzando los mecanismos de defensa contra amenazas cibernéticas cada vez más sofisticadas.

Proveedores de Nube Preferidos

A continuación, preguntamos a los profesionales de la ciberseguridad sobre su uso actual y futuro de los proveedores de la nube, para comprender mejor la dinámica cambiante del mercado dentro del ecosistema de la nube. Microsoft Azure continúa liderando el mercado: el 62 % de las organizaciones de nuestra encuesta utilizan actualmente sus servicios, seguido por Amazon Web Services (AWS) con un 54 %. Esto indica una fuerte preferencia por estos gigantes de las nubes establecidos.

Los resultados de la encuesta también resaltan un interés significativo en la adopción futura en todos los proveedores, particularmente Oracle Cloud y Google Cloud Platform, con un 27% y un 25% de los encuestados planeando adoptar estos servicios, respectivamente. Esto sugiere una adopción de la nube cada vez más diversa.

► ¿Qué proveedores de IaaS en la nube utiliza actualmente o planea utilizar en el futuro? (Seleccione todas las que correspondan)



Navegando las Barreras de la Adopción de la Nube

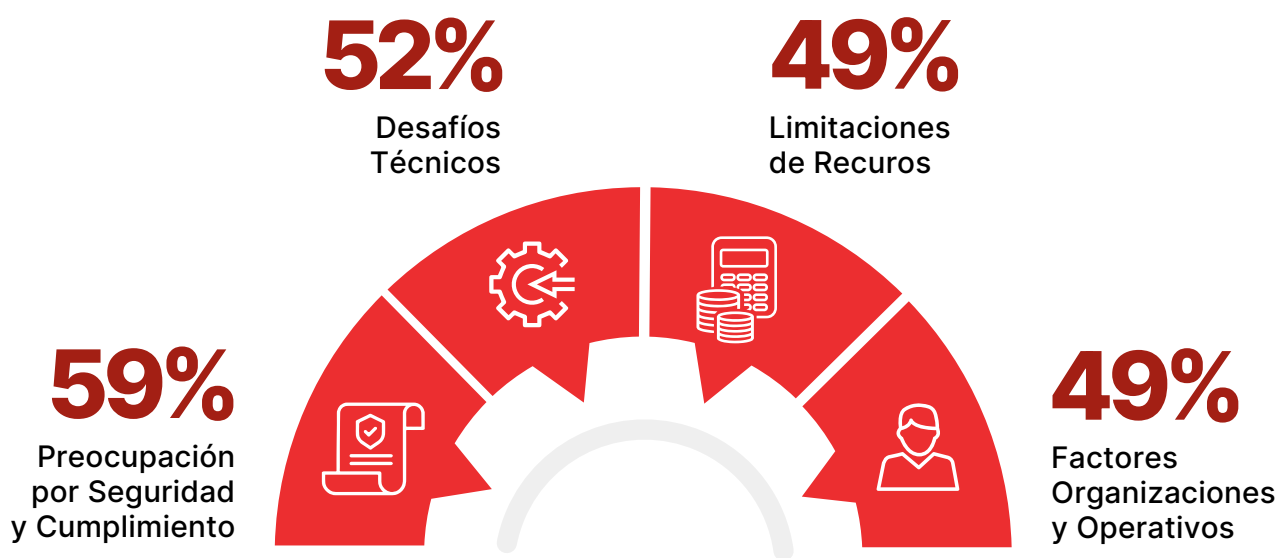
Identificar y comprender las barreras para una adopción más rápida y generalizada de la nube es esencial para que las organizaciones naveguen mejor por las complejidades de la transición a soluciones basadas en la nube.

Las preocupaciones por la seguridad y el cumplimiento están a la vanguardia, y el 59% de los encuestados lo identifican como una barrera principal. Esto resalta la importancia de garantizar que la seguridad y el cumplimiento sean un elemento integral de la adopción de la nube.

Los desafíos técnicos le siguen de cerca con un 52%, lo que destaca que la facilidad de adopción de la nube no está exenta de desafíos.

El 49% de los encuestados cita limitaciones de recursos, incluida la falta de experiencia del personal y limitaciones presupuestarias, lo que subraya la necesidad de una inversión adecuada en recursos humanos y financieros para respaldar las iniciativas en la nube. Las barreras organizativas y operativas (49%) subrayan que la computación en la nube no es sólo una nueva tecnología, sino también un nuevo modelo operativo que ofrece métodos de trabajo innovadores y requiere la aceptación de la dirección para abordar la posible resistencia al cambio.

► **¿Cuáles son las principales barreras para la adopción de la nube en su organización?**
(Seleccione todas las que correspondan)



Las respuestas adicionales incluyen:

El servicio en la nube preocupa al 28% | Cuestiones y legalidades relacionadas con el proveedor 27%

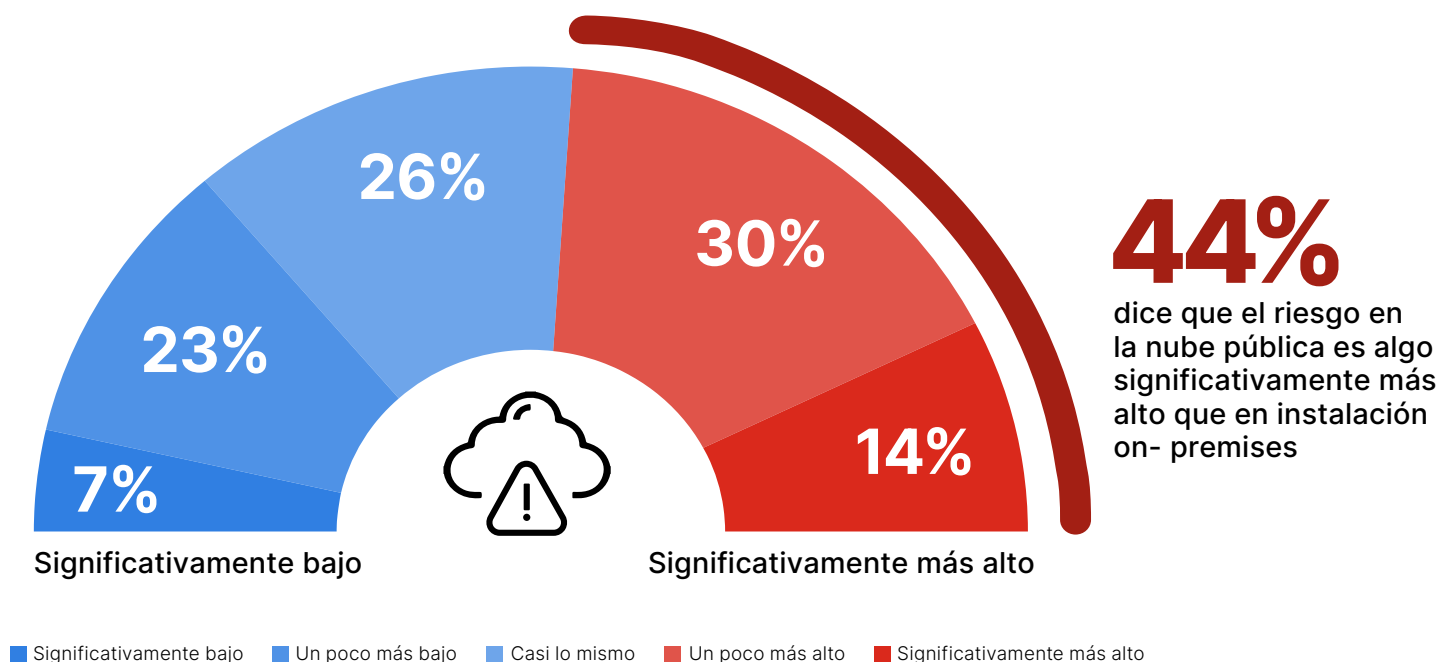
Percepciones de los Riesgos de Seguridad en la Nube

La evaluación del riesgo de violaciones de seguridad en entornos de nube pública revela preocupaciones importantes sobre los riesgos y desafíos de seguridad únicos asociados con la computación en la nube, en comparación con los entornos locales.

Un 44% combinado de los encuestados percibe que el riesgo de violaciones de seguridad en entornos de nube pública es mayor que en entornos de TI locales tradicionales, un 30% lo considera algo mayor y un 14% lo considera significativamente mayor.

Por el contrario, el 30% de los participantes considera que el riesgo es menor en entornos de nube pública, lo que indica confianza en las medidas y avances de seguridad de los proveedores de nube. Un notable 26% de los encuestados cree que el riesgo sigue siendo el mismo, lo que sugiere que si bien la nube introduce nuevas dinámicas, los desafíos fundamentales de seguridad persisten en diferentes ambientes.

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



La nube pública ofrece a las organizaciones la oportunidad de adoptar un enfoque de seguridad proactivo y automatizado. Adoptar una mentalidad de seguridad por diseño ofrece a las organizaciones la capacidad de mitigar riesgos de manera efectiva y capitalizar la escalabilidad, flexibilidad e innovación que ofrece la nube.

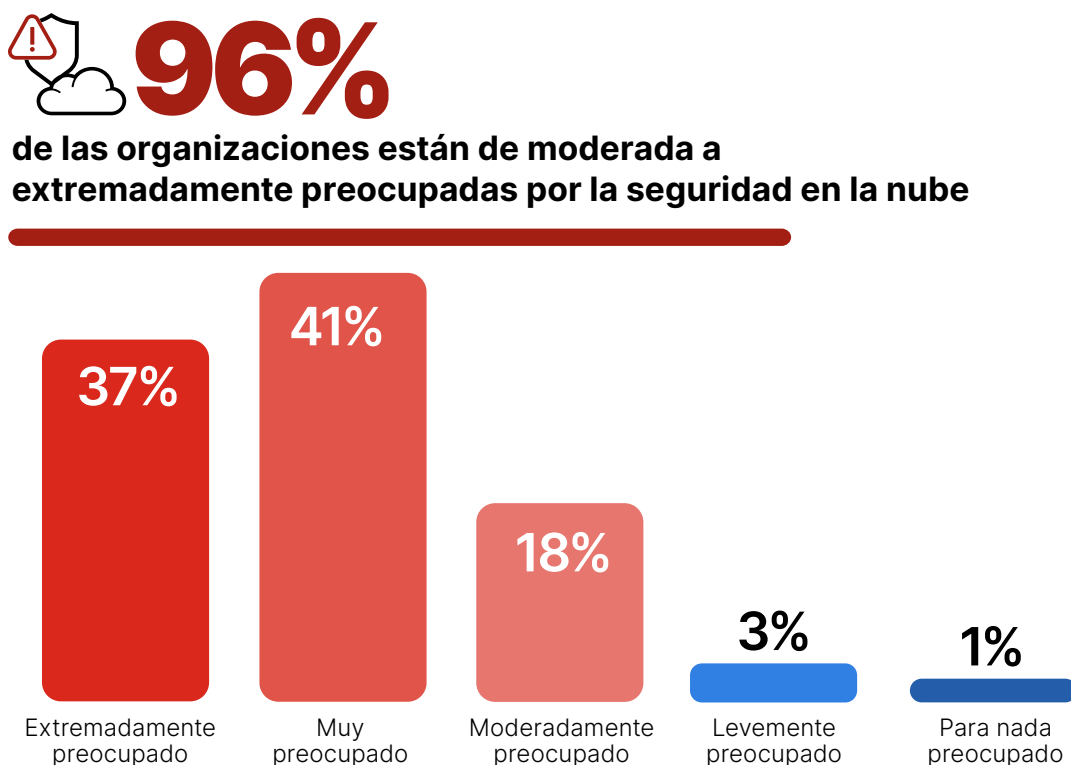
Preocupaciones de Seguridad en la Nube

El nivel de preocupación con respecto a la seguridad de la nube pública es un indicador crítico de la percepción y la preparación de la comunidad de ciberseguridad para abordar riesgos y amenazas potenciales.

A pesar de la creciente adopción de la nube, las preocupaciones sobre la seguridad de la nube no muestran signos de mejorar: una mayoría significativa del 96% expresa altos niveles de preocupación, el 37% está extremadamente preocupado y el 41% muy preocupado por la seguridad de la nube pública. El alto grado de preocupación por la ciberseguridad, que se ha mantenido constante a lo largo de los años, actúa como una barrera importante para una adopción más rápida de la nube, a medida que las organizaciones lidian con los riesgos percibidos y las complejidades de proteger los entornos de nube. Solo una pequeña fracción (22%) reporta preocupación moderada o nula, lo que indica un fuerte consenso sobre la importancia de medidas de seguridad sólidas en las implementaciones de la nube pública.

Estos datos se alinean con el hallazgo anterior en el que un 44% combinado de los encuestados percibió un mayor riesgo de violaciones de seguridad en las nubes públicas en comparación con los entornos locales tradicionales. Esto refuerza el hecho de que, si bien la computación en la nube ofrece numerosos beneficios y crece rápidamente, la seguridad sigue siendo una preocupación primordial.

► ¿Qué tan preocupado está por la seguridad de las nubes públicas?



Para abordar estas preocupaciones, las organizaciones no solo deben mantener un enfoque de seguridad desde el diseño, sino también invertir en monitoreo continuo, inteligencia sobre amenazas y capacidades de respuesta a incidentes específicas para entornos de nube. Adoptar soluciones de seguridad de vanguardia y fomentar colaboraciones sólidas con proveedores de nube puede ayudar a mitigar el riesgo percibido y las preocupaciones asociadas con la nube pública, garantizando una infraestructura de nube segura y resiliente.

Desafíos en las Operaciones de Seguridad en la Nube

La gestión de las operaciones diarias de seguridad en la nube presenta un desafío multifacético para las organizaciones, que requiere un delicado equilibrio entre factores tecnológicos, de procedimiento y humanos. La seguridad y la privacidad de los datos emergen como la principal preocupación: el 58% de los encuestados destaca la importancia crítica de proteger la información confidencial y prevenir las fugas de datos en la nube. Esto subraya la importancia de prácticas sólidas de cifrado y gobernanza de datos. La gestión de la configuración ocupa el segundo lugar con un 55%, lo que refleja la complejidad y los riesgos potenciales asociados con las configuraciones de la nube, ya que una sola configuración incorrecta puede exponer a las organizaciones a importantes riesgos de seguridad.

El control de acceso y la gestión de identidad es otro desafío importante, citado por el 54% de los participantes, enfatizando la necesidad de un control estricto sobre el acceso y los privilegios de los usuarios para evitar el acceso no autorizado. La detección y respuesta a amenazas (50%) y la seguridad de endpoints (45%) indican además la lucha continua para identificar y mitigar las amenazas de seguridad en tiempo real y proteger la gran cantidad de dispositivos que acceden a los servicios en la nube. La gestión de políticas y cumplimiento (45%) y la gestión de la seguridad en la nube (45%) resaltan las dificultades para garantizar políticas de seguridad consistentes en todos los entornos y alinear las características de seguridad de la nube con las soluciones on-premises.

► **¿Cuáles son sus principales desafíos en la gestión de las operaciones diarias de seguridad en la nube?**
(Seleccione todas las que correspondan)



Para afrontar estos desafíos en las operaciones de seguridad en la nube, las organizaciones deben priorizar una estrategia de seguridad unificada que aproveche la automatización, el análisis avanzado y las plataformas de seguridad integradas para optimizar la seguridad de los datos, la aplicación de políticas, la gestión del acceso y la detección y respuesta a amenazas. Hacer hincapié en el desarrollo de habilidades de seguridad nativas de la nube dentro de los equipos y fomentar una cultura de concientización sobre la seguridad puede mejorar aún más la capacidad de una organización para gestionar las operaciones de seguridad en la nube de forma eficaz.

Las respuestas adicionales incluyen:
TI en la Sombra y uso de aplicaciones no autorizadas 36 % | Integración y automatización de la nube 35% | Agilidad y Complejidad Operacional 32% | Recurso Asignación 30% | Prácticas de DevSecOps 28%

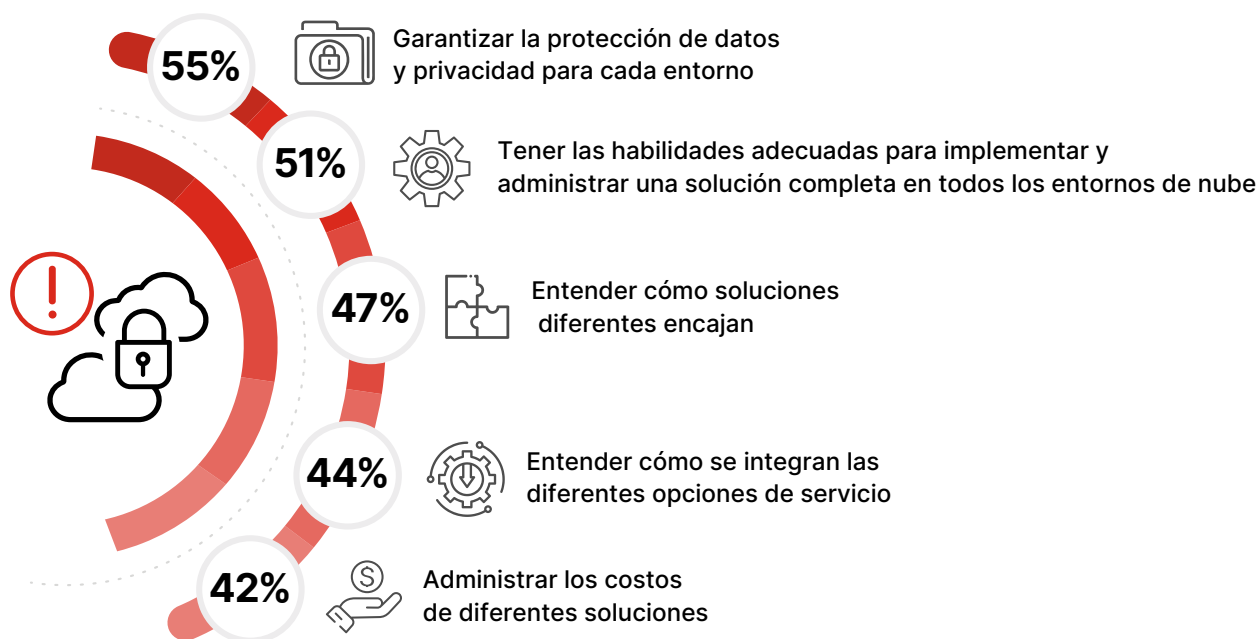
Desafíos de Seguridad en Múltiples Nubes

Los entornos de múltiples nubes aumentan significativamente la complejidad y los desafíos de proteger las cargas de trabajo en la nube. Garantizar la protección de datos y la privacidad en cada entorno se identifica como el desafío de seguridad multinube más importante, y el 55% de los encuestados lo destacó como una preocupación. Esto se alinea con el énfasis anterior en la seguridad y privacidad de los datos como cuestiones operativas críticas, lo que subraya la mayor complejidad cuando los datos se dispersan en múltiples entornos de nube.

Tener las habilidades adecuadas para implementar y administrar soluciones en todos los entornos de nube es un desafío importante para el 51% de los participantes, lo que refleja la necesidad previamente señalada de contar con experiencia en seguridad nativa de la nube para navegar de manera efectiva en el multifacético panorama de seguridad de la nube. Comprender cómo encajan las diferentes soluciones y comprender las opciones de integración de servicios son desafíos críticos para el 47% y el 44% de los encuestados, respectivamente.

Estas preocupaciones resaltan las complejidades de lograr una integración e interoperabilidad perfectas entre diversos entornos de nube, un factor crucial para mantener una seguridad sólida y una eficiencia operativa. El desafío de gestionar los costos de diferentes soluciones, citado por el 42% de los encuestados, refleja aún más el acto de equilibrio operativo y financiero requerido en una estrategia de múltiples nubes.

► ¿Cuáles son sus mayores desafíos para asegurar entornos multinube? (Seleccione todas las que correspondan)



Para abordar eficazmente estos desafíos, las organizaciones deben aprovechar soluciones de seguridad integradas que ofrezcan visibilidad y control en entornos de múltiples nubes, respaldando estándares consistentes de privacidad y protección de datos. Hacer hincapié en las asociaciones con proveedores que brindan capacidades integrales de seguridad multinube y fomentar el desarrollo de habilidades puede ayudar a las empresas a superar la complejidad de proteger las arquitecturas multinube. Este enfoque no solo mitiga los desafíos identificados, sino que también aprovecha todo el potencial de los entornos de múltiples nubes para mejorar la agilidad, la escalabilidad y la innovación.

Las respuestas adicionales incluyen:

Proporcionar acceso fluido a los usuarios según sus credenciales 38% | Pérdida de visibilidad y control 37% | Seleccionar el conjunto adecuado de servicios 36% Mantenerse al día con la tasa de cambio 33%

Brecha de Talento en Ciberseguridad

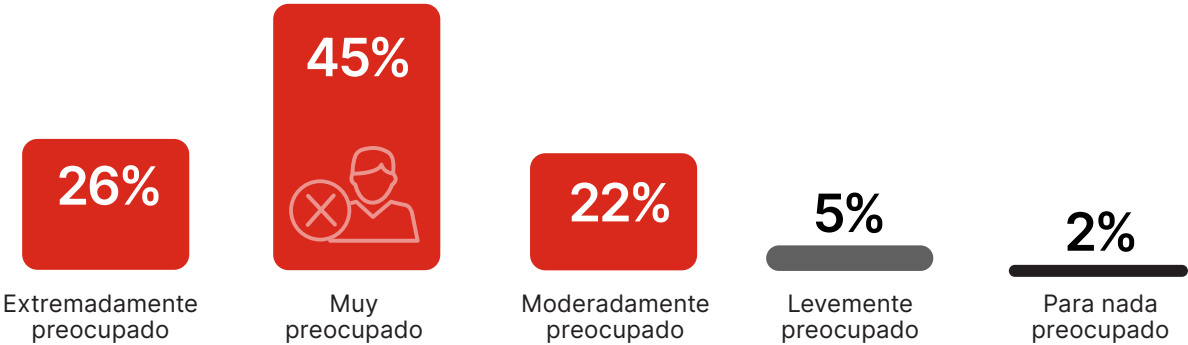
Haciéndose eco de los desafíos destacados en la protección de entornos multinube, la actual escasez de profesionales capacitados capaces de proteger entornos multinube complejos se destaca como un problema continuo y crítico de la industria.

Un abrumador 93% de los encuestados expresa preocupación por la escasez en toda la industria de profesionales calificados en ciberseguridad. Esta considerable aprensión refleja la aguda conciencia de la brecha entre la creciente demanda de talento calificado en ciberseguridad y la fuerza laboral disponible, una brecha que exacerba las vulnerabilidades de seguridad y los desafíos operativos en un panorama cibernético cada vez más complejo.

► **¿Qué tan preocupado está usted por la escasez de personal calificado en toda la industria?
¿Profesionales de ciberseguridad?**

93%

de las organizaciones están de moderada a extremadamente Preocupadas sobre la escasez de profesionales calificados en ciberseguridad



Un rotundo 74% de los encuestados confirma que su organización está experimentando actualmente una escasez de talento en ciberseguridad. Este hallazgo cuantifica hasta qué punto la escasez de habilidades está afectando las operaciones diarias e iniciativas estratégicas dentro de las organizaciones.

► **¿Su Organización está experimentando escasez de talento en Ciberseguridad?**



Para mitigar el impacto de la constante escasez de habilidades en ciberseguridad, las organizaciones deben considerar un enfoque multifacético que incluya el fomento de asociaciones con instituciones académicas para canalizar nuevos talentos e invertir en programas de capacitación y desarrollo para cultivar el talento interno y adaptarse a las demandas cambiantes de la seguridad en la nube. Las organizaciones también deberían considerar adoptar soluciones de seguridad unificadas que reemplacen las soluciones de múltiples puntos, incorporando inteligencia artificial y reduciendo la complejidad operativa para cerrar la brecha de habilidades y al mismo tiempo mejorar la detección de amenazas, las capacidades de respuesta y la postura general de seguridad.

Habilidades Críticas en Ciberseguridad

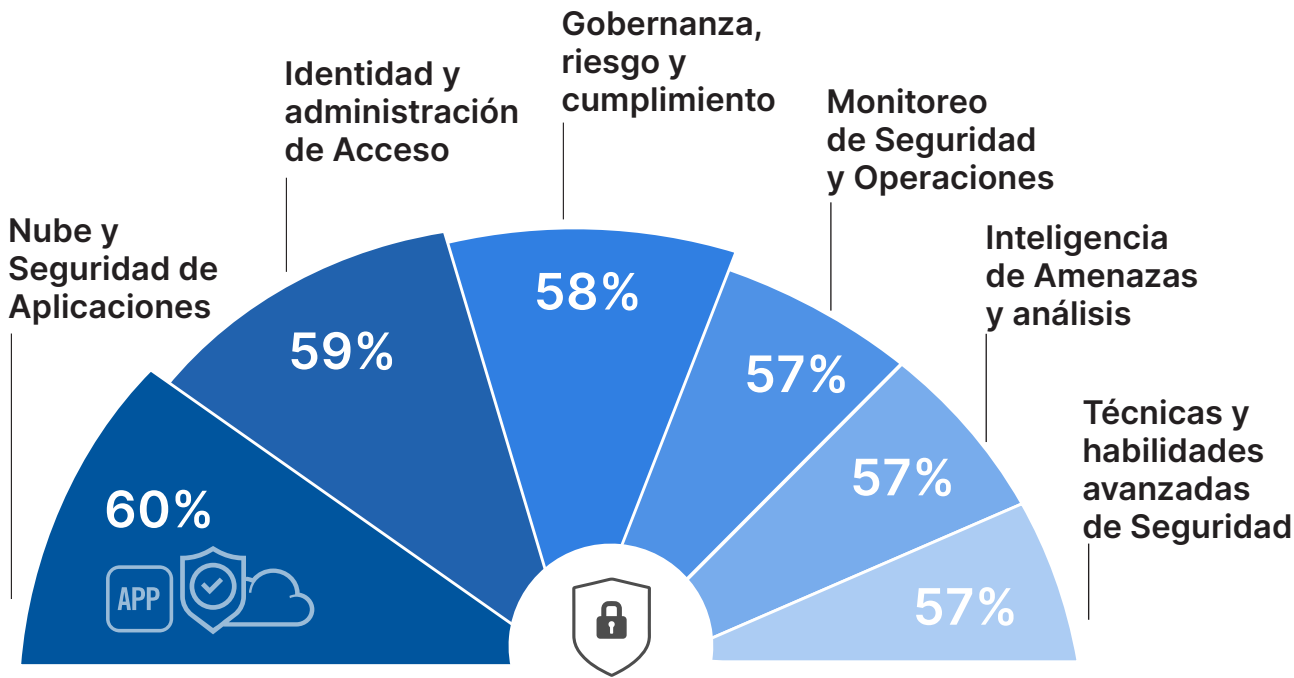
En el contexto de la pronunciada escasez de talento en ciberseguridad que enfrentan las organizaciones, preguntamos sobre las habilidades específicas de ciberseguridad que se consideran más críticas para abordar los desafíos de seguridad actuales.

Las habilidades de seguridad de aplicaciones y nube ocupan el primer lugar, y el 60% de los encuestados destaca su importancia crítica.

Esto subraya la migración acelerada a los servicios en la nube y la necesidad de prácticas de seguridad sólidas en el desarrollo y la implementación de aplicaciones. Siguiéndola de cerca, el 59% de las organizaciones identifican la gestión de identidades y accesos (IAM) como esencial, lo que refleja la creciente complejidad de proteger el acceso de los usuarios en entornos de TI cada vez más distribuidos.

El 58 % de los encuestados reconoce la gobernanza, el riesgo y el cumplimiento (GRC) como una habilidad importante, lo que subraya el papel esencial del cumplimiento normativo y los marcos de gestión de riesgos en el panorama actual de las amenazas cibernéticas. Operaciones y monitoreo de seguridad, inteligencia sobre amenazas y habilidades técnicas avanzadas de seguridad (todos al 57%) demuestran un énfasis casi igual en la detección proactiva de amenazas, la comprensión de los ciberadversarios y el aprovechamiento de tecnologías avanzadas para una postura de seguridad sólida.

► ¿Cuáles son las habilidades de seguridad más importantes requeridas en su organización?
(Seleccione todas las que correspondan)



Las respuestas adicionales incluyen:
Respuesta a incidentes y análisis forense 55% | Comunicación y estrategia 39% | Formación y sensibilización 38%

Tendencias del Presupuesto de Seguridad en la Nube

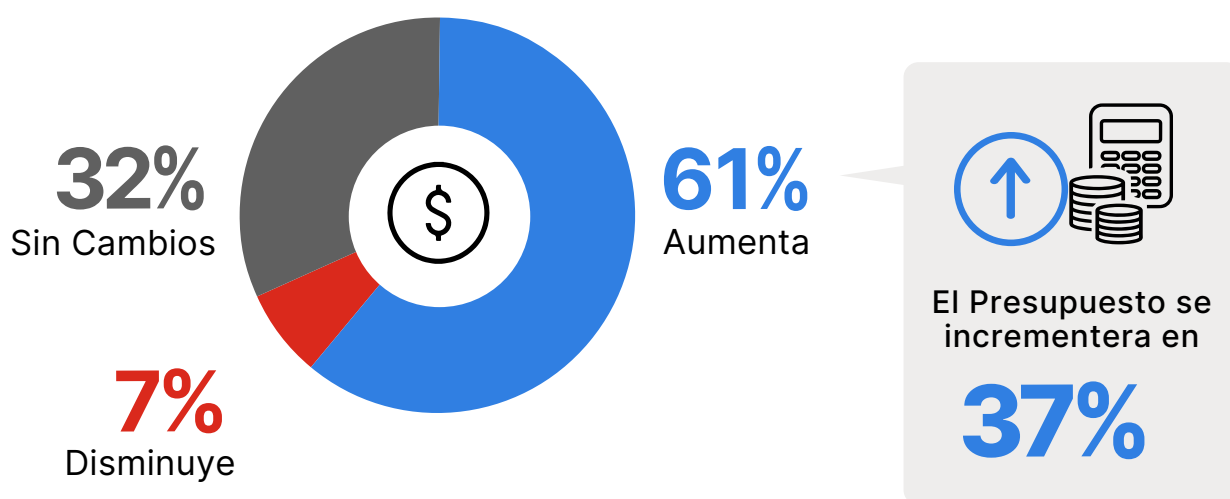
La asignación de recursos a la seguridad de la nube es un indicador crítico de las prioridades organizacionales y de la importancia percibida de la protección de la infraestructura de la nube frente a la evolución de las amenazas cibernéticas y los avances tecnológicos.

Un significativo 61% de los encuestados anticipa un aumento en su presupuesto de seguridad en la nube durante los próximos 12 meses. Esta mayoría sustancial indica un fuerte reconocimiento de los crecientes desafíos de ciberseguridad y la necesidad de mejorar las medidas de seguridad en los entornos de nube, lo que impulsó que el presupuesto de seguridad en la nube aumentara en un 37%.

La voluntad de invertir hasta un 37% más en seguridad en la nube refleja la comprensión de que los mecanismos de defensa sólidos son esenciales para salvaguardar los datos confidenciales y mantener el cumplimiento de los estándares regulatorios en un panorama empresarial cada vez más centrado en la nube.

Mientras tanto, un tercio de las organizaciones (32%) espera que su presupuesto de seguridad en la nube se mantenga sin cambios. Sólo una pequeña fracción, el 7%, proyecta una disminución en su presupuesto de seguridad en la nube.

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

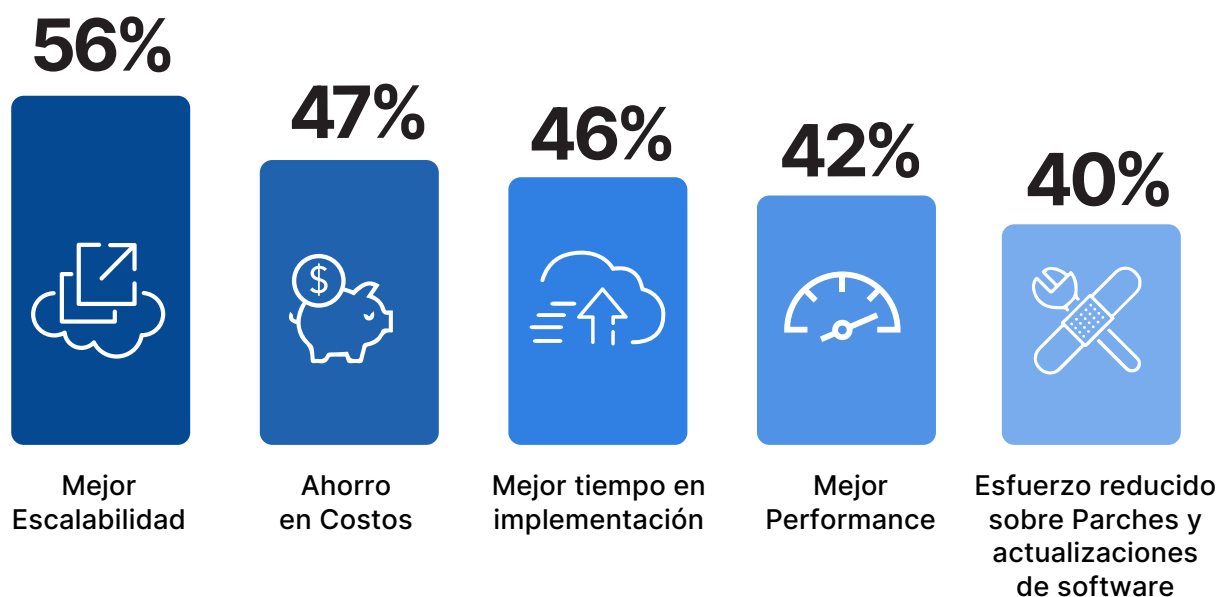


Dada la tendencia predominante hacia una mayor inversión en seguridad en la nube, las organizaciones deberían asignar estratégicamente recursos adicionales a áreas de mayor riesgo y potencial impacto, como la detección avanzada de amenazas, la gestión de identidades y accesos, y la automatización de la seguridad. Este enfoque no sólo prepara a las empresas para combatir las amenazas cibernéticas sofisticadas, sino que también mejora su postura general de seguridad al aprovechar las últimas innovaciones tecnológicas en seguridad en la nube.

Adoptar Soluciones de Seguridad Basadas en la Nube

La decisión de adoptar soluciones de seguridad basadas en la nube está impulsada por una variedad de factores que se alinean con los objetivos organizacionales de agilidad, eficiencia y protección mejorada. La necesidad de una mejor escalabilidad, reconocida por el 56% de los encuestados, destaca la capacidad de la nube para adaptarse dinámicamente a las demandas fluctuantes. Muy cerca, el ahorro de costos y una implementación más rápida, con un 47% y un 46% respectivamente, subrayan los beneficios económicos y operativos que atraen a las organizaciones hacia las soluciones de seguridad en la nube. El rendimiento mejorado (42%) y la reducción de los esfuerzos manuales para aplicar parches y actualizaciones de software (40%) catalizan aún más el cambio hacia soluciones de seguridad basadas en la nube, especialmente a la luz de la perenne escasez de habilidades en ciberseguridad.

► ¿Cuáles son los principales impulsores para considerar soluciones de seguridad basadas en la nube? (Seleccione todas las que correspondan)



Las organizaciones que estén considerando soluciones de seguridad basadas en la nube deben priorizar la escalabilidad, la eficiencia de costos y la implementación rápida para capitalizar las ventajas operativas y económicas de la nube. Centrarse en soluciones que ofrecen una gestión de políticas optimizada y un cumplimiento continuo puede mejorar aún más las posturas de seguridad, garantizando la resiliencia frente a las amenazas y los panoramas regulatorios en evolución.

Las respuestas adicionales incluyen:

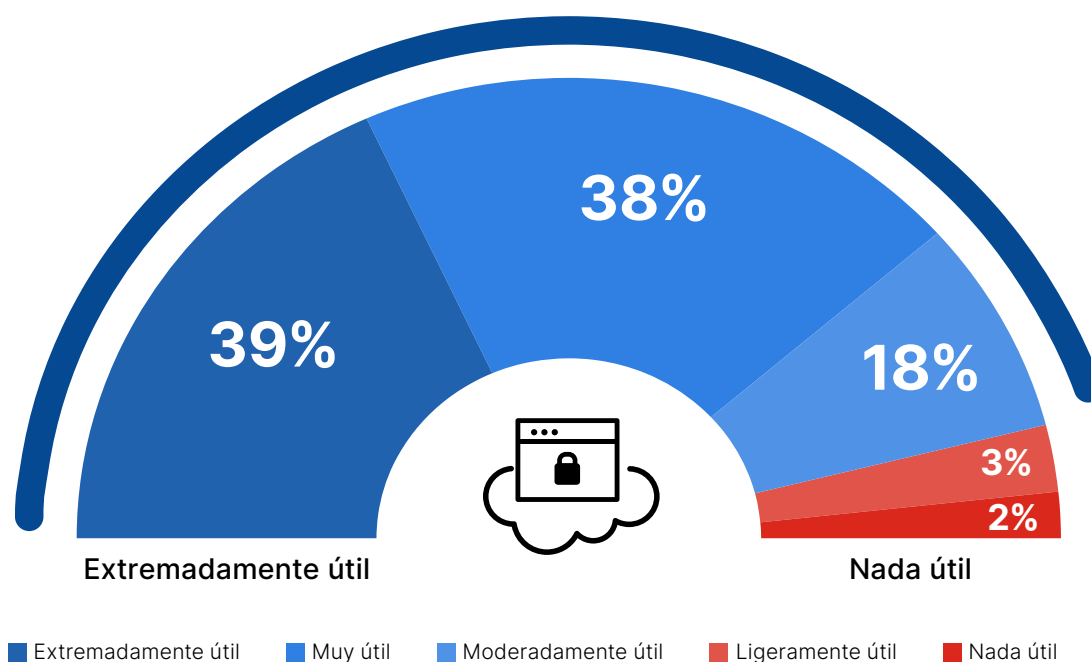
Gestión de políticas más sencilla 39% | Mejor tiempo de actividad 38% | Cumplir con las expectativas de cumplimiento de la nube 34% | Mejor visibilidad de la actividad del usuario y el comportamiento del sistema 33% | Necesidad de acceso seguro a aplicaciones desde cualquier ubicación 32% | Nuestros datos/cargas de trabajo residen en la nube 28% | Reducción de huella de electrodomésticos en sucursales 27%

Plataforma Unificada de Seguridad en la Nube

Dada la complejidad, los dolores de cabeza operativos y los desafíos de habilidades ya destacados, no sorprende que las organizaciones estén buscando una plataforma de seguridad unificada para optimizar y consolidar la gestión de la seguridad en diversos entornos de nube. Un abrumador 95% de los encuestados confirma que tener una plataforma de este tipo sería ventajoso para proteger los datos de manera consistente y completa en toda la huella de la nube.

- ¿Qué utilidad tendría tener una única plataforma de seguridad en la nube con un único panel donde podría configurar todas las políticas necesarias para proteger los datos de manera consistente y de manera integral en toda su huella en la nube?

95% de los profesionales consideran que el uso de una única plataforma de seguridad en la nube con un único dashboard es de moderada a extremadamente útil.



Esta demanda de una plataforma de seguridad en la nube única e integrada refleja el cambio de la industria hacia la consolidación de plataformas, impulsada por la mejora de la eficacia de la seguridad, una integración más sencilla y una reducción de los gastos generales de gestión. Es el único enfoque eficaz para abordar la brecha de talento en ciberseguridad y mitigar ataques cada vez más sofisticados y automatizados. Una plataforma unificada de este tipo alivia la carga operativa de navegar por múltiples interfaces de seguridad y mejora la postura general de seguridad mediante la aplicación consistente de políticas y una visibilidad integral en todos los entornos de nube.

Adoptar la Nube de Forma Segura: Estrategias Esenciales de Seguridad en la Nube

En el panorama actual de la nube en rápida evolución, adoptar una postura sólida de seguridad en la nube es imperativo para organizaciones de todos los tamaños. Esta guía describe las mejores prácticas esenciales para proteger sus entornos de nube, desde unificar plataformas de seguridad hasta invertir en habilidades especializadas, diseñadas para proteger contra las sofisticadas amenazas del mañana.



ADOPTAR UNA PLATAFORMA DE SEGURIDAD UNIFICADA:

Centralizar el control de seguridad y la visibilidad en todos los entornos de nube para optimizar las operaciones y mejorar la visibilidad, una estrategia preferida por el 95% de las organizaciones.



ENFATIZAR LA SEGURIDAD AGNÓSTICA DE LA NUBE:

Dado que el 78% utiliza entornos híbridos o de múltiples nubes, es crucial desarrollar estrategias que aborden los desafíos únicos de estos entornos y garanticen políticas y cumplimiento de seguridad consistentes.



AUTOMATIZAR LA GESTIÓN DE POLÍTICAS Y CUMPLIMIENTO:

Implementar sistemas para automatizar y optimizar las políticas de seguridad en entornos de nube y cumplir constantemente con los requisitos normativos.



PRIORIZAR LA PROTECCIÓN DE DATOS:

Implementar una gobernanza y cifrado de datos sólidos para salvaguardar la información confidencial en todos los servicios en la nube, abordando el desafío de seguridad mencionado por el 58% de las organizaciones.



MEJORAR LA GESTIÓN DE LA CONFIGURACIÓN:

Administrar activamente las configuraciones de la nube para evitar configuraciones erróneas y reducir la exposición a vulnerabilidades de seguridad.



FORTALECER EL CONTROL DE ACCESO:

Emplear una gestión estricta de identidades y accesos para implementar los principios de Confianza Cero y reducir el riesgo de acceso no autorizado.



IMPULSAR LA DETECCIÓN Y RESPUESTA A LAS AMENAZAS:

Aprovechar el análisis avanzado y las capacidades de respuesta automatizada para identificar y mitigar amenazas en tiempo real.



INVERTIR EN HABILIDADES DE SEGURIDAD NATIVAS DE LA NUBE:

Dado que el 93% expresa gran preocupación por la escasez de habilidades en ciberseguridad, fomentar el desarrollo de la experiencia en seguridad específica de la nube dentro de su equipo para navegar por el complejo panorama de seguridad de la nube de manera más efectiva.

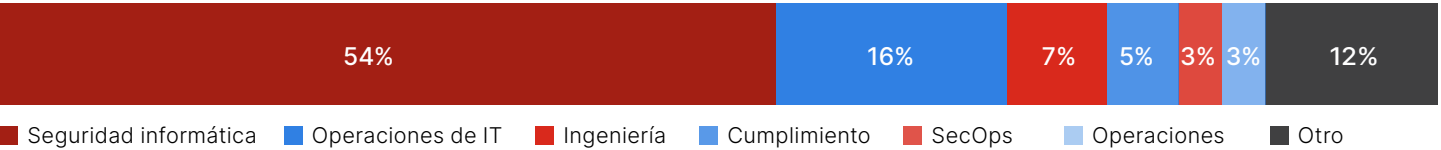
Metodología y Demografía

El Informe de seguridad en la nube 2024 se basa en una encuesta global integral de 927 profesionales de la ciberseguridad realizada en febrero de 2024, para descubrir 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 están priorizando los líderes de ciberseguridad de TI en sus pasar a la nube. Los encuestados van desde ejecutivos técnicos hasta profesionales de seguridad de TI, lo que representa una muestra representativa equilibrada de organizaciones de distintos tamaños en múltiples industrias.

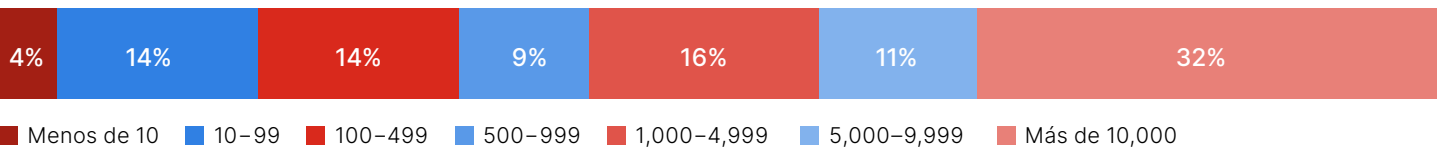
NIVEL DE CARRERA



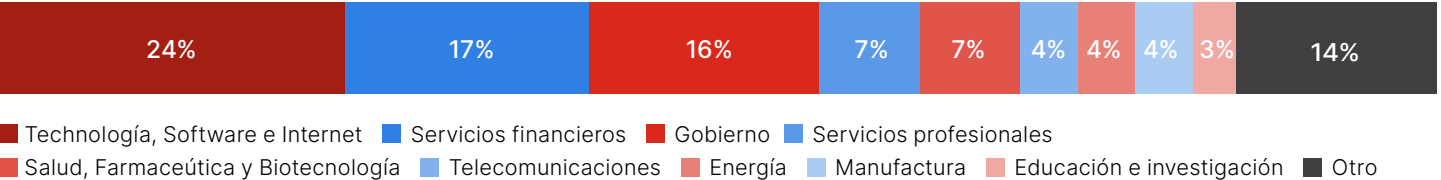
DEPARTAMENTO



TAMAÑO DE LA EMPRESA



INDUSTRIA



Reutilización de contenidos

Fomentamos la reutilización de datos, gráficos y textos publicados en este informe bajo los términos de esta [Licencia Internacional Creative Commons Attribution 4.0](#). Eres libre de compartir y hacer uso comercial de este trabajo siempre y cuando atribuyas el informe según lo estipulado en los términos de la licencia. Por ejemplo: “Informe de seguridad en la nube de 2024 elaborado por Cybersecurity Insiders y Fortinet”.



Fortinet (NASDAQ: FTNT) asegura las mayores empresas y servicios proveedores y organizaciones gubernamentales de todo el mundo. Fortinet brinda a nuestros clientes visibilidad y control completos en todo la superficie de ataque en expansión y el poder de enfrentarse a requisitos de rendimiento cada vez mayores en la actualidad y en el futuro. Sólo la plataforma Fortinet Security Fabric puede abordar los desafíos de seguridad más críticos y proteger los datos en todo la infraestructura digital, ya sea en redes, aplicaciones, multinube, o entornos de borde. Fortinet ocupa el puesto número 1 como la empresa con la mayoría de los dispositivos de seguridad enviados en todo el mundo y más de 730.000 clientes que confían en Fortinet para proteger sus negocios.

www.fortinet.com

Cybersecurity

I N S I D E R S

Cybersecurity Insiders reúne a más de 600.000 profesionales de seguridad informática y proveedores de tecnología de clase mundial para facilitar la resolución inteligente de problemas y colaboración para abordar los desafíos de ciberseguridad más críticos de la actualidad.

Nuestro enfoque se centra en crear y seleccionar contenido único que eduque e informe a los profesionales de la ciberseguridad sobre las últimas novedades en ciberseguridad, tendencias, soluciones y mejores prácticas. A partir de estudios de investigación exhaustivos,

y reseñas imparciales de productos hasta guías electrónicas prácticas, seminarios web atractivos y artículos educativos: estamos comprometidos a proporcionar recursos que proporcionen respuestas basadas en evidencia a los complejos desafíos de ciberseguridad actuales.

Contáctenos hoy para saber cómo Cybersecurity Insiders puede ayudarlo a destacarse en un mercado abarrotado e impulsar la demanda, la visibilidad de la marca y el liderazgo intelectual presencia.

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