



EL ESTADO DE LA SEGURIDAD NATIVA EN LA NUBE 2022

Grupo 3:

- Nardy Cachipuendo
- Ariel Guaña
- Cristofer Paucar
- Juan Rengifo
- Nathaly Slmba

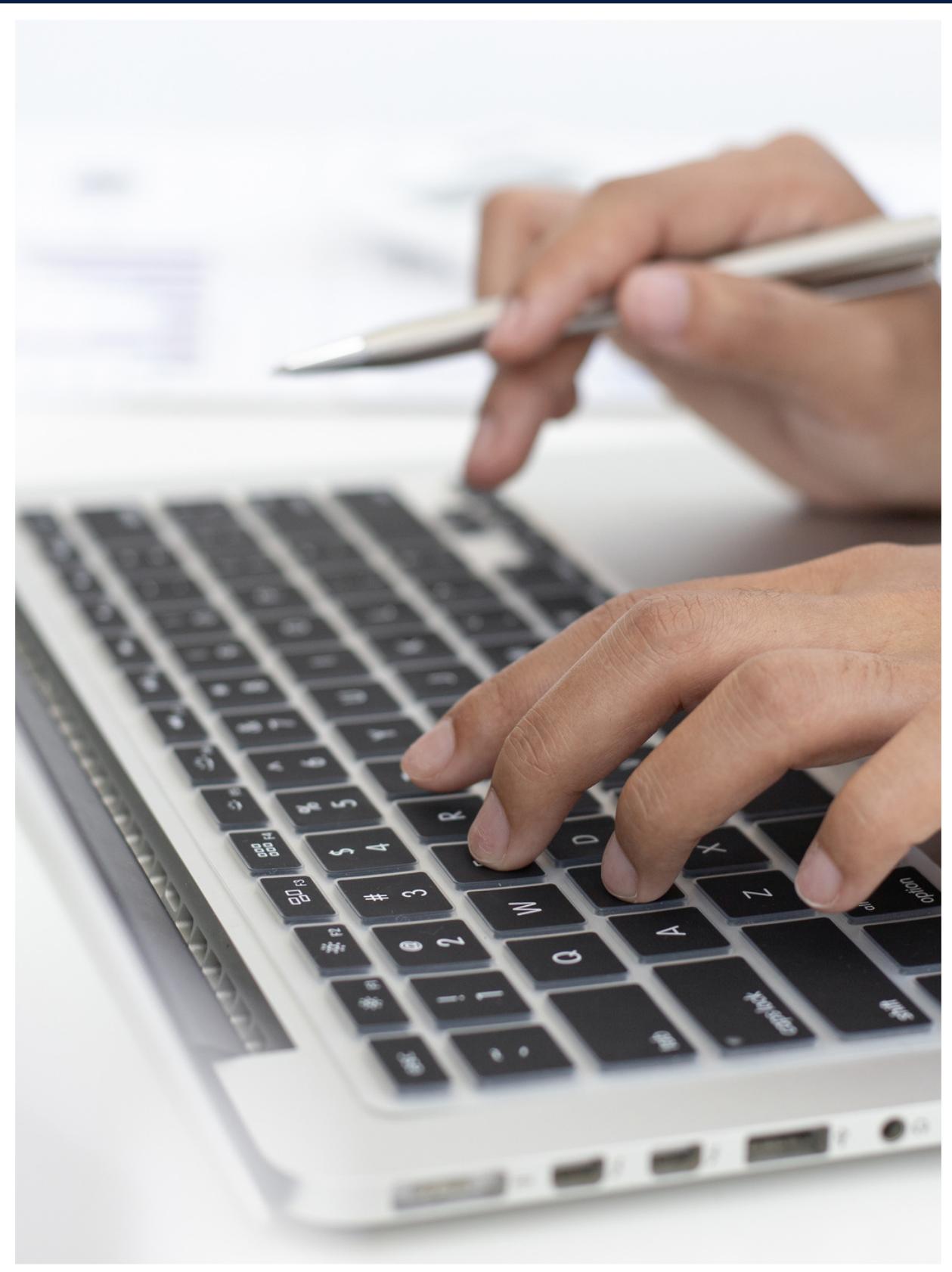
Profesor: Ing. Juan Herrera
Fecha: 1/12/2023

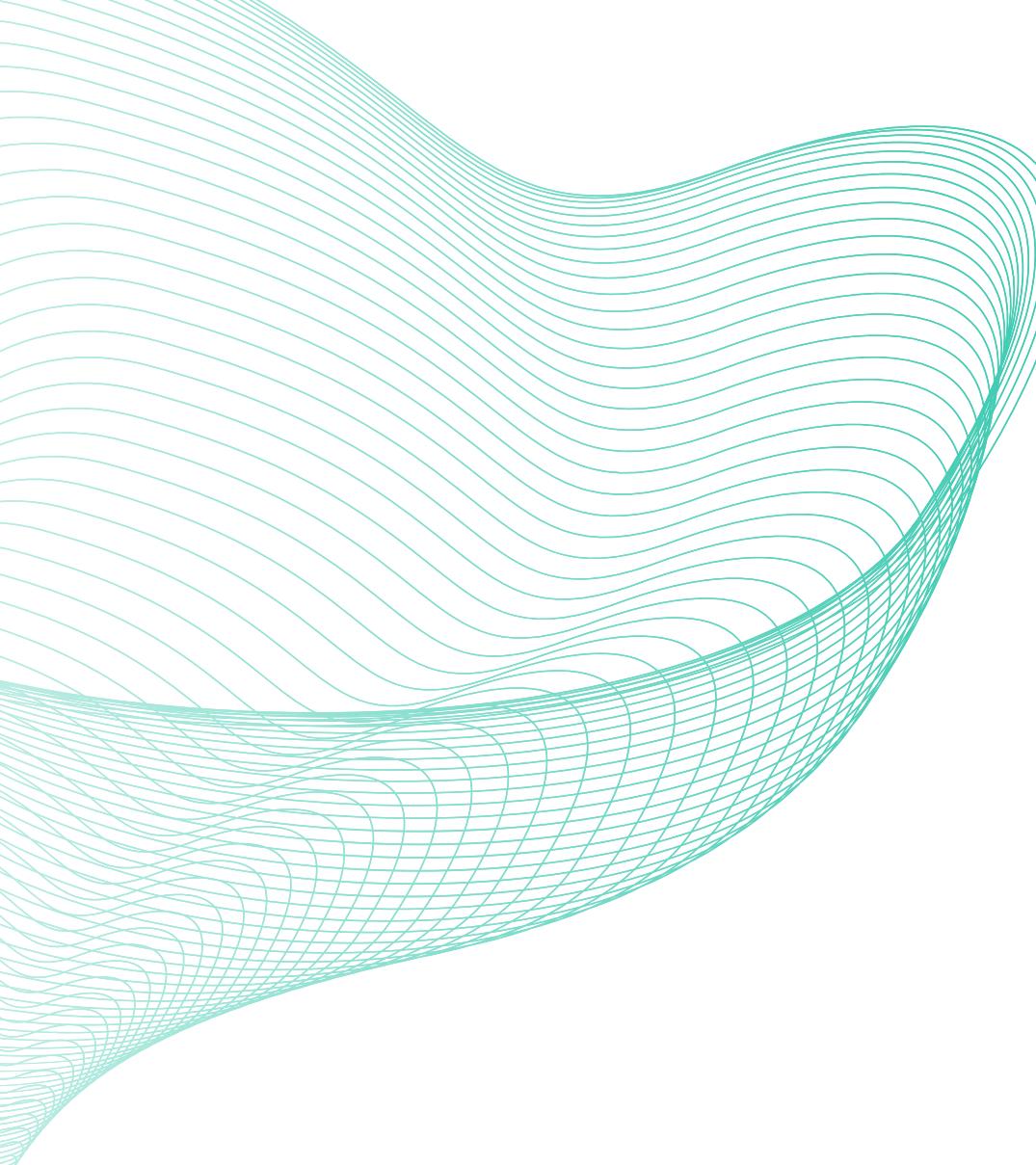
Índice

- Introducción
- Crecimiento de la nube en pandemia
- Desafíos de seguridad al migrar a la nube
- La expansión rápida en la nube
- Panorama en la Nube en 2022
- Amenazas comunes a la seguridad en la nube

Introducción

- Encuesta a más de 3,000 personas en todo el mundo sobre sus estrategias, presupuestos y experiencias en la adopción de la nube.
- La pandemia de COVID-19 ha influido en la expansión de la nube.
- Adoptantes Moderados, Expandidores Rápidos y Usuarios Establecidos.





Expansión y Estrategia en la Nube

- Las organizaciones expandieron su uso de la nube en más del 25%, pero enfrentaron desafíos.
- Muchas organizaciones gastaron menos en la nube.
- Servicio (PaaS), enfoques serverless, Contenedores (Cass)

Postura de Seguridad y Fricción

- Las organizaciones con una sólida postura de seguridad tienen menos fricción de seguridad.
- Operaciones de seguridad de primer nivel ven mayores beneficios en productividad y satisfacción laboral.
- La mayoría de las organizaciones reconocen una postura de seguridad débil.

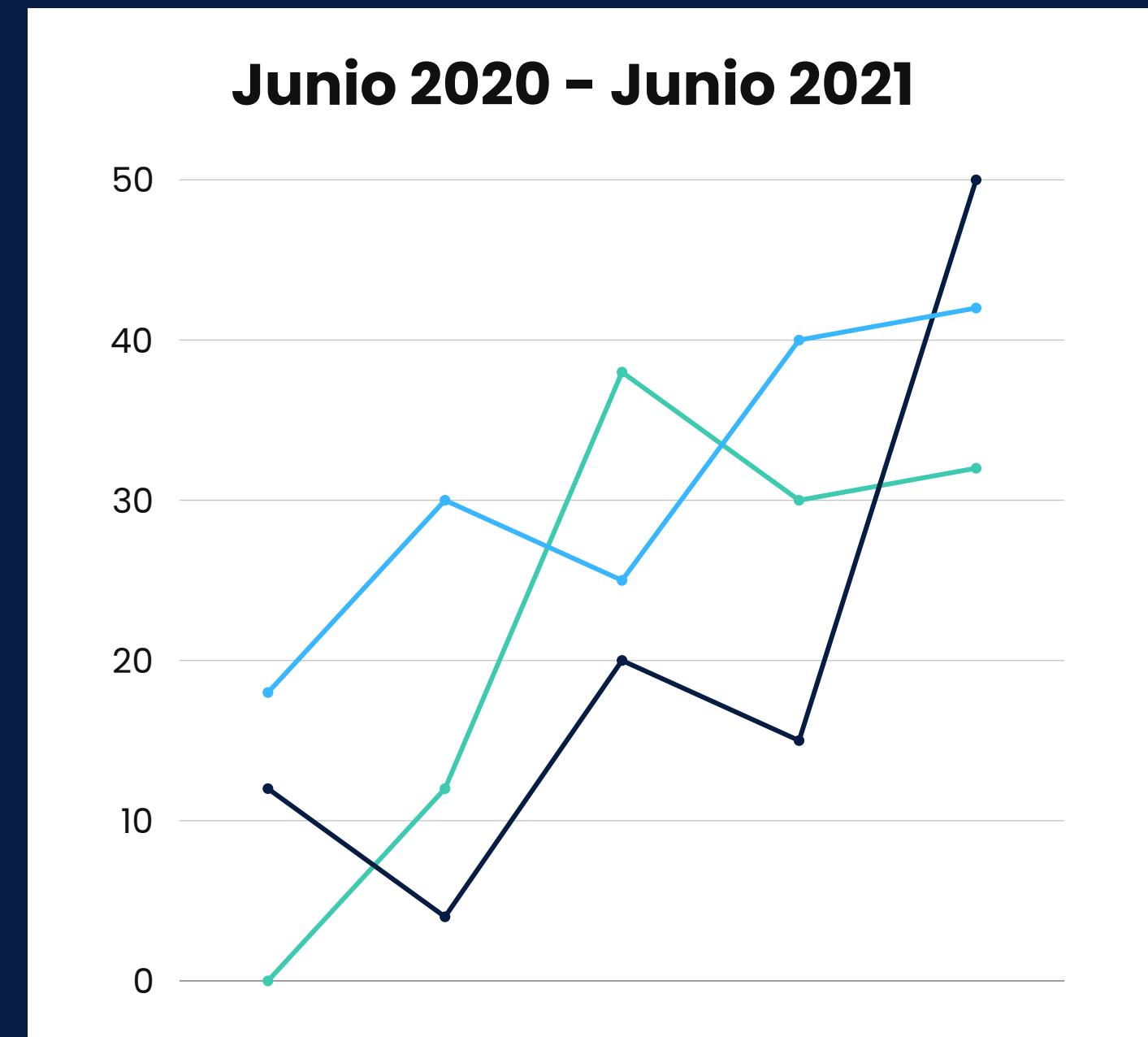
Este informe aborda las preocupaciones más actuales de la comunidad de seguridad nativa en la nube

Factores de Seguridad

- Las organizaciones utilizan menos herramientas de seguridad, buscando más capacidades en menos proveedores.
- La automatización de seguridad está fuertemente vinculada a una baja fricción.
- Metodologías DevSecOps es el indicador principal de una seguridad de alta calidad.

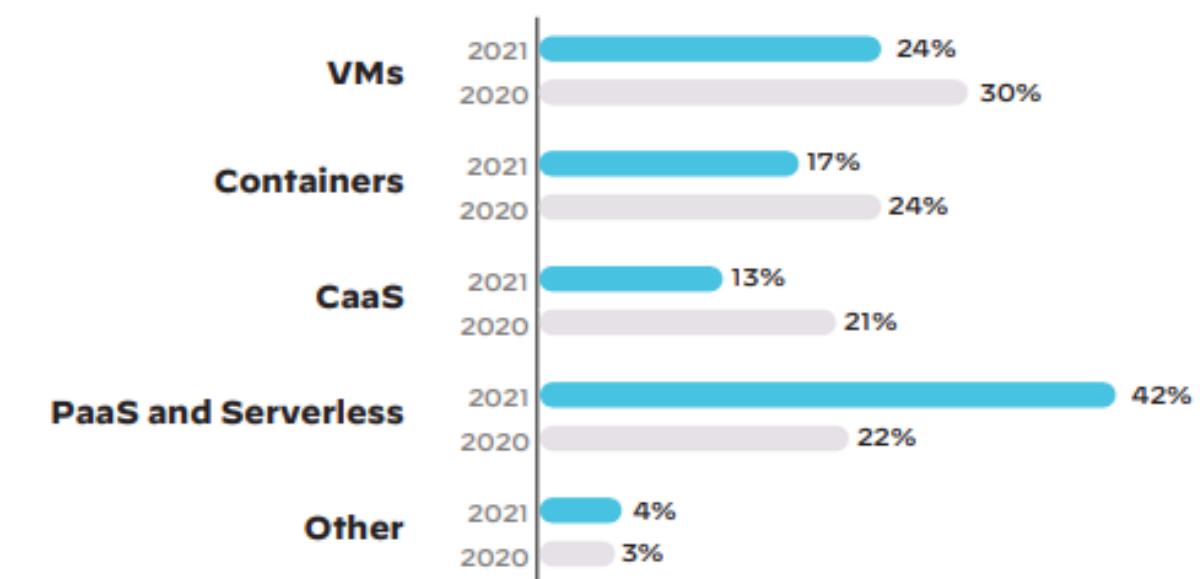
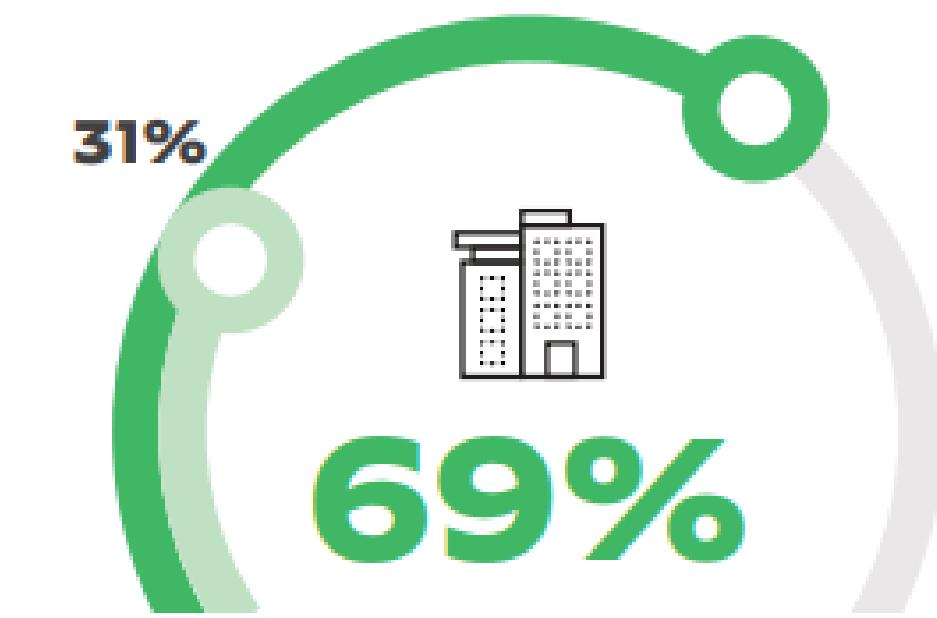
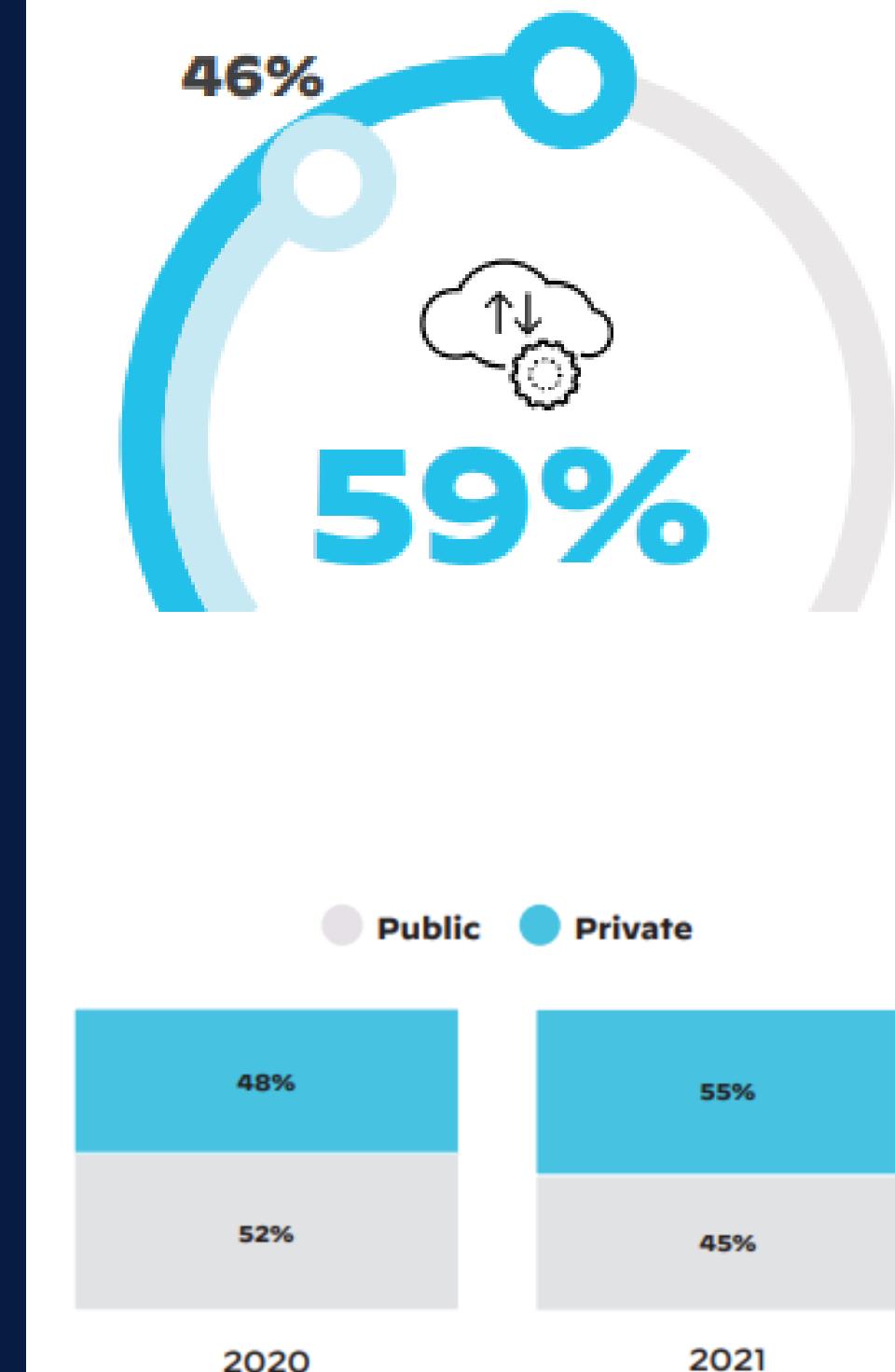
El impacto del Covid-19

- Las organizaciones se vieron afectadas por cambios drásticos en la demanda de servicios en la nube.
- Esta rápida transición también conllevó un aumento en los ciberataques (implementar controles de seguridad automatizados).
- A pesar de la continua migración hacia la nube, se destaca la necesidad urgente de integrar controles de seguridad sólidos y automatizados en todo el ciclo de vida del desarrollo en la nube.

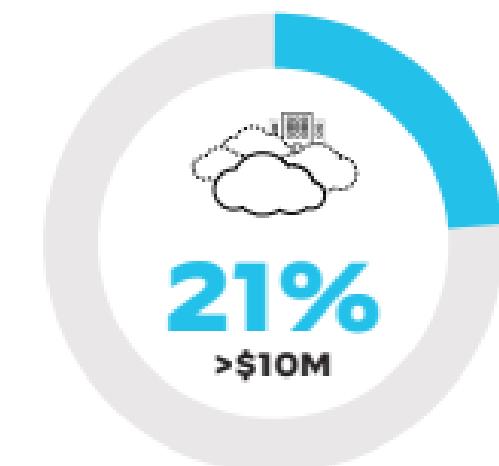
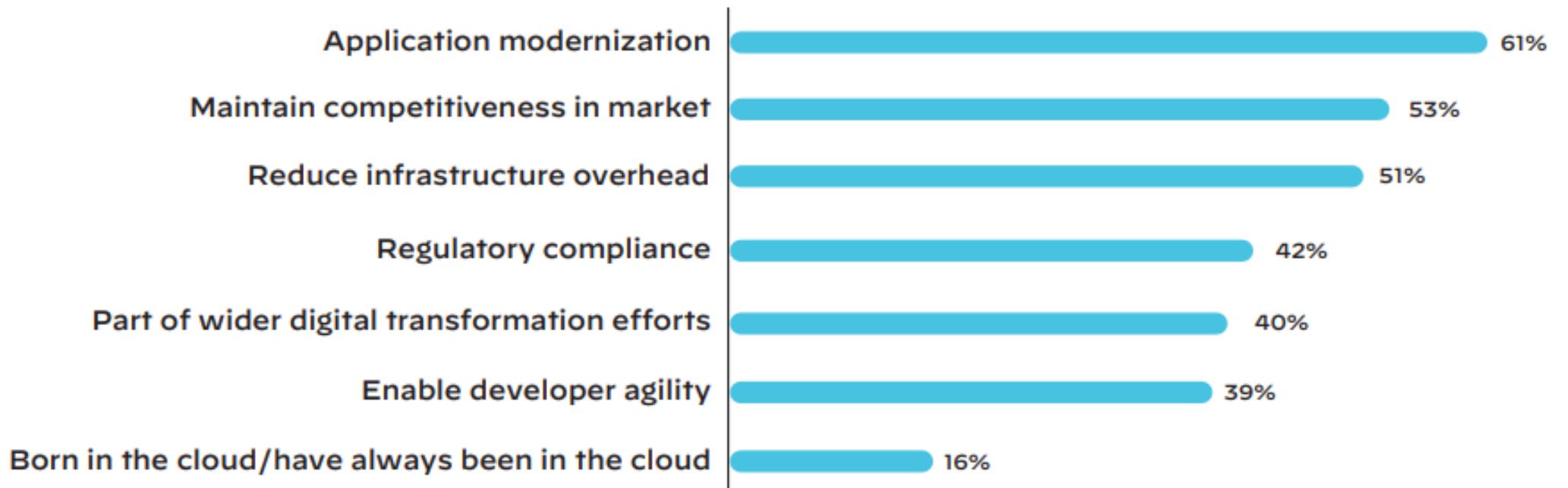


Crecimiento de la nube en pandemia

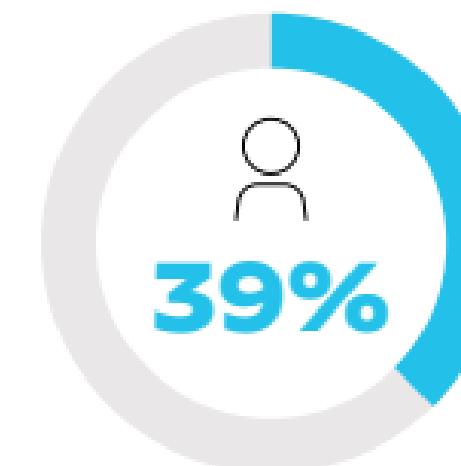
- Durante la pandemia, hubo un aumento significativo en la adopción de la nube.
- El 69% de las organizaciones ahora alojan más de la mitad de sus cargas de trabajo en la nube, en comparación con solo el 31% en 2020.
- En promedio, se espera que las organizaciones alojen el 68% de sus cargas de trabajo en la nube en dos años.
- Aumento del uso de alojamiento privado para cargas de trabajo en la nube, con un promedio del 55%
- Estrategias como PaaS y enfoques serverless han ganado terreno al permitir a los equipos de desarrollo colocar aplicaciones en la nube sin necesariamente construir y escalar la infraestructura al mismo tiempo



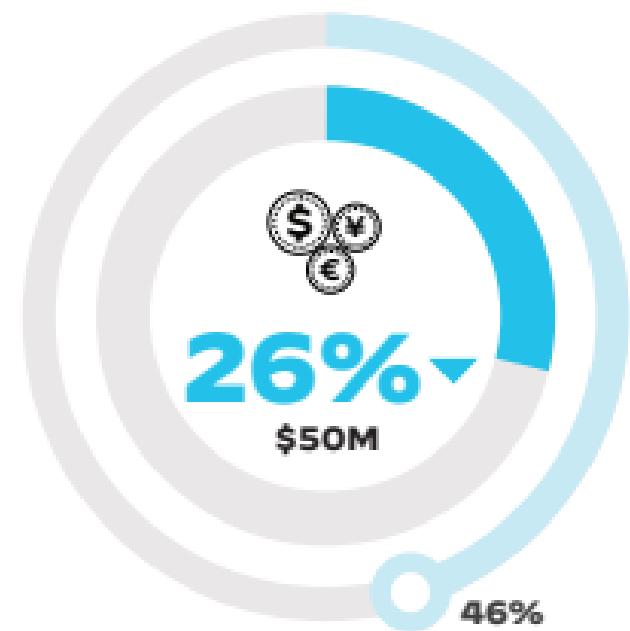
- El crecimiento de las capacidades en la nube de las organizaciones fue impulsado por motivadores estratégicos de negocios, como la modernización de aplicaciones, el mantenimiento de la competitividad y el control de los costos de infraestructura.
- La flexibilidad y agilidad que ofrece la nube permiten a las organizaciones avanzar a un ritmo cada vez más rápido.
- En 2021, un 39% de las organizaciones gastaron menos de \$10 millones en su nube, un aumento del 16% desde 2020. Mientras que solo un 26% gastó más de \$50 millones, una disminución del 17% desde 2020.



In 2020, 21% of organizations dedicated less than \$10M toward their cloud.



In 2021, 39% of respondents fall in that category.



Orgs with cloud budgets over \$50M dropped from 46% to 26%.

Casi la mitad (47%) de los encuestados de Estados Unidos reportan una postura de seguridad fuerte o muy fuerte, más alto en comparación con otros países.

Alemania reportó el porcentaje más alto de automatización de procesos de seguridad (40%).

Japón reportó el aumento más significativo en el uso de arquitectura Serverless (57%) en los próximos 24 meses, más que cualquier otra arquitectura.

En Brasil, casi la mitad (48%) de los encuestados esperan que sus empresas tengan entre el 76% y el 100% de sus cargas de trabajo en la nube en los próximos dos años, lo que muestra un movimiento hacia la adopción de la nube.

El Reino Unido utiliza más herramientas de código abierto como su proveedor principal para la seguridad en la nube que cualquier otro país encuestado.

Desafíos de seguridad al migrar a la nube

1.- Crecimiento en el Uso de la Nube:

- Las organizaciones han ampliado rápidamente su uso de la nube en el último año.

2.- Desafíos Principales:

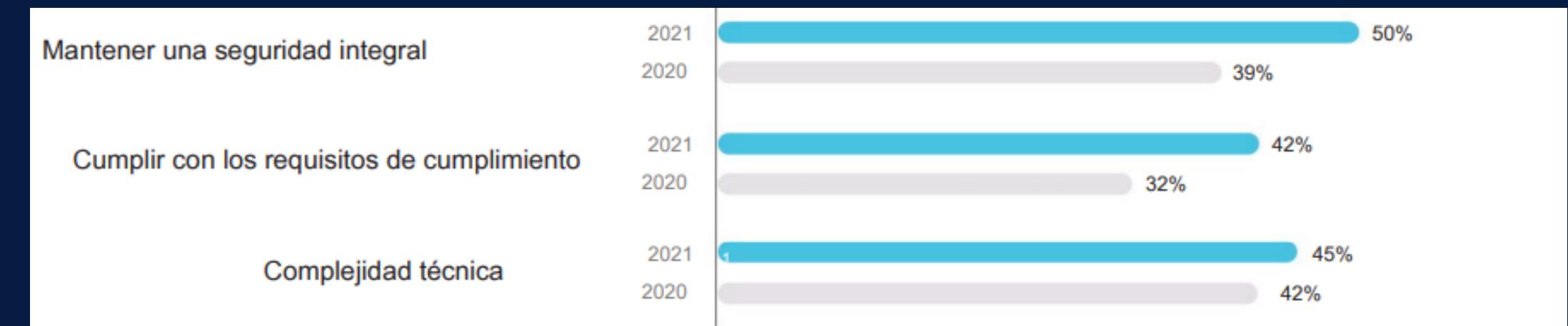
- A pesar del crecimiento en el uso de la nube, las organizaciones siguen enfrentando los mismos desafíos principales que el año anterior.
- Los desafíos destacados son la seguridad y el cumplimiento integrales, así como la complejidad técnica.

3.- Presupuestos:

- Aunque los presupuestos generales de la nube disminuyeron, los presupuestos destinados a la seguridad en la nube se mantuvieron estables.
- Esto sugiere que, aunque las organizaciones redujeron el gasto en la nube en general, no comprometieron los recursos destinados a la seguridad.

4.- Valor de Proteger la Nube:

- La estabilidad en los presupuestos de seguridad en la nube indica que las empresas comprenden la importancia de proteger sus entornos en la nube para aprovechar al máximo sus beneficios.

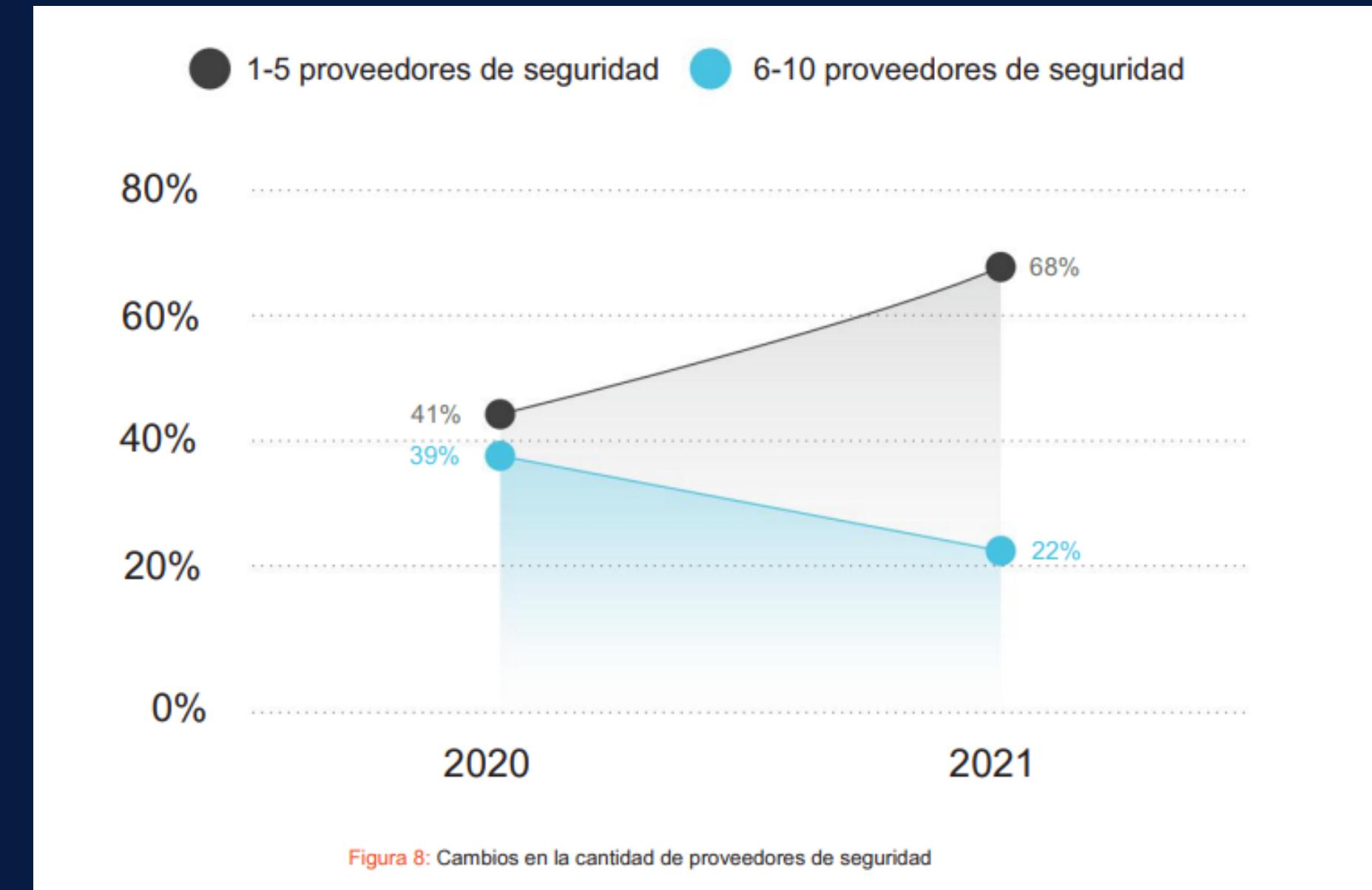


5.- Equipos de Seguridad en la Nube:

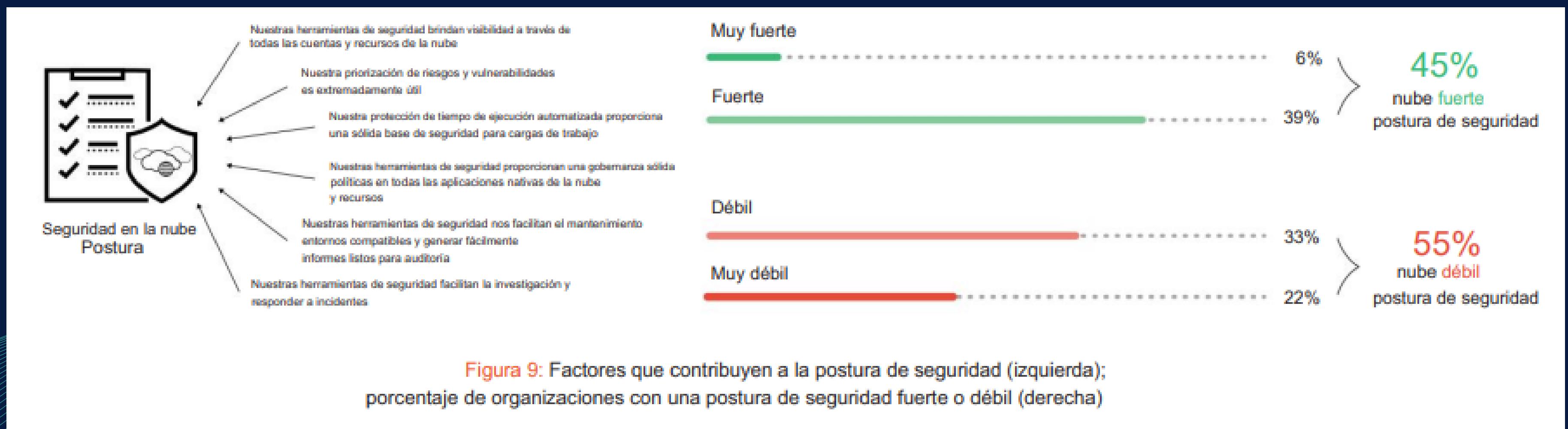
- Durante la pandemia, las empresas han expandido sus equipos de seguridad en la nube.
- El 53% de las organizaciones informaron tener un equipo de seguridad de más de 30 personas, en comparación con el 41% del año anterior.

6.- Consolidación de Proveedores:

- Las empresas han consolidado sus proveedores de seguridad en la nube a medida que expanden sus entornos de nube.
- Se observa un aumento del 27% en el número de organizaciones que utilizan solo de uno a cinco proveedores de seguridad.
- Aquellas que utilizan de seis a diez proveedores han disminuido un 17% desde el año pasado.



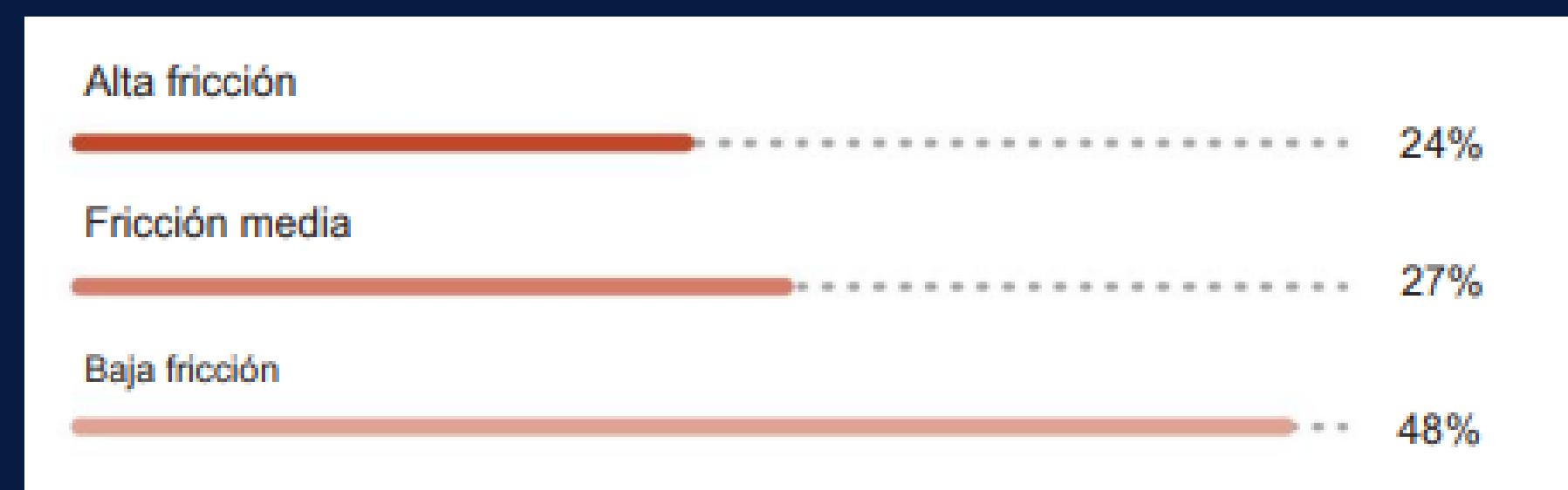
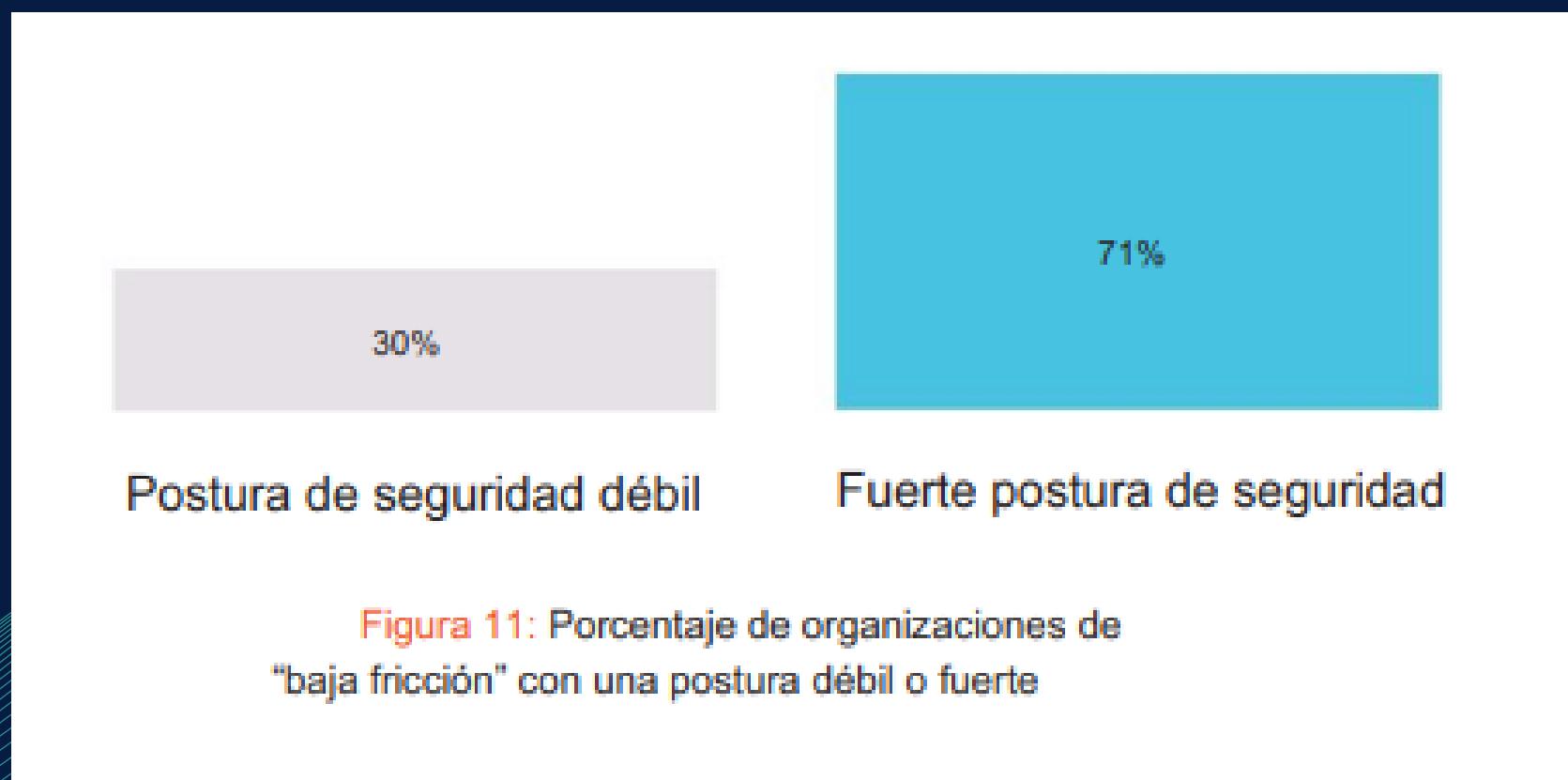
- El objetivo de esta presentación es analizar los cambios en el panorama de seguridad en la nube, centrandonos en la consolidación de proveedores, la cantidad de herramientas utilizadas y los atributos de seguridad organizacional.
- Examinaremos cómo estas tendencias afectan el rendimiento general de las organizaciones y exploraremos factores clave para el éxito en la seguridad en la nube.



Consolidación de Proveedores y Herramientas:

1.- Reducción de Proveedores:

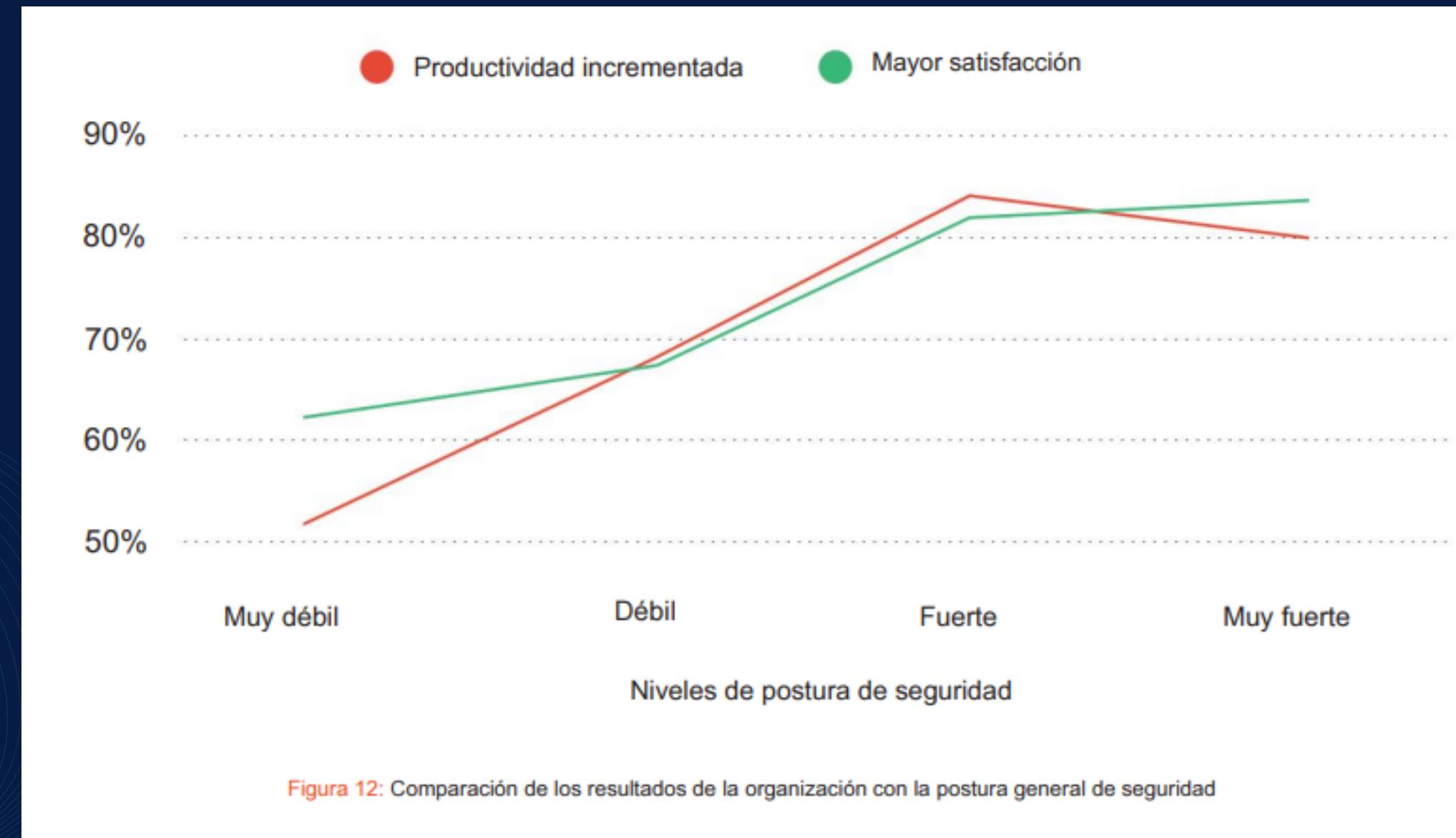
- Las empresas han reducido la cantidad de proveedores de seguridad, pero han realizado cambios mínimos en la cantidad de herramientas utilizadas año tras año.
- La definición de proveedores se enfoca en empresas que protegen las nubes, y la consolidación sugiere una búsqueda de eficiencia.



Consolidación de Proveedores y Herramientas:

2.- Uso de Herramientas de Seguridad:

- Casi el 75% de las organizaciones utilizan 10 o menos herramientas de seguridad, indicando una consolidación para abordar diversas capacidades.
- Advertencia para el 28% que utiliza más de 20 herramientas, ya que esto puede aumentar el riesgo y requerir esfuerzos adicionales.



Consolidación de Proveedores y Herramientas:

3.- Relación entre Herramientas y Proveedores:

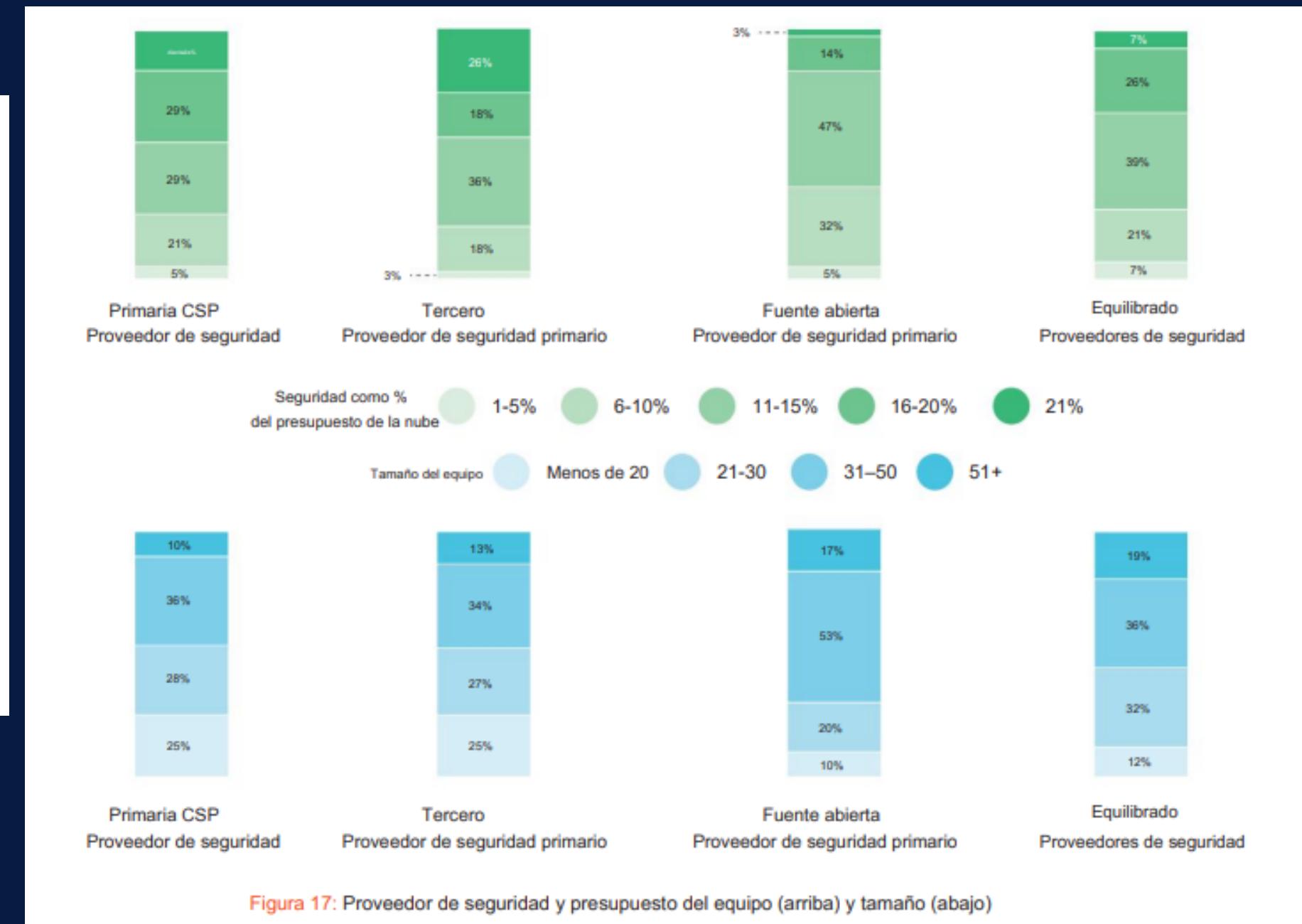
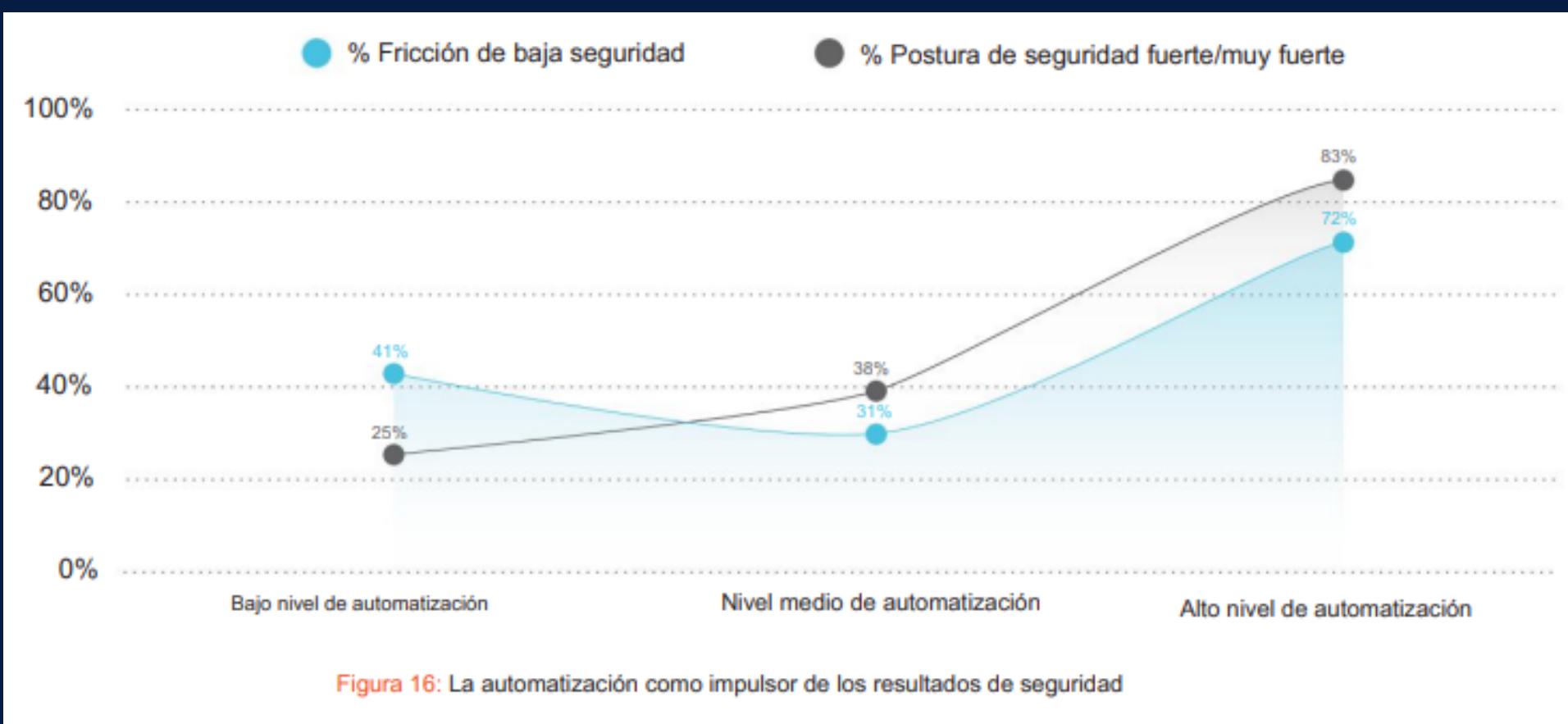
- El 91% de las organizaciones que usan más de 20 herramientas utilizan seis o más proveedores.
- Equipos más grandes (49% con más de 50 empleados) administran estas herramientas para garantizar la seguridad de las cargas de trabajo en la nube.



Atributos Organizacionales y Factores de Éxito:

4.- Postura de Seguridad y Fricción:

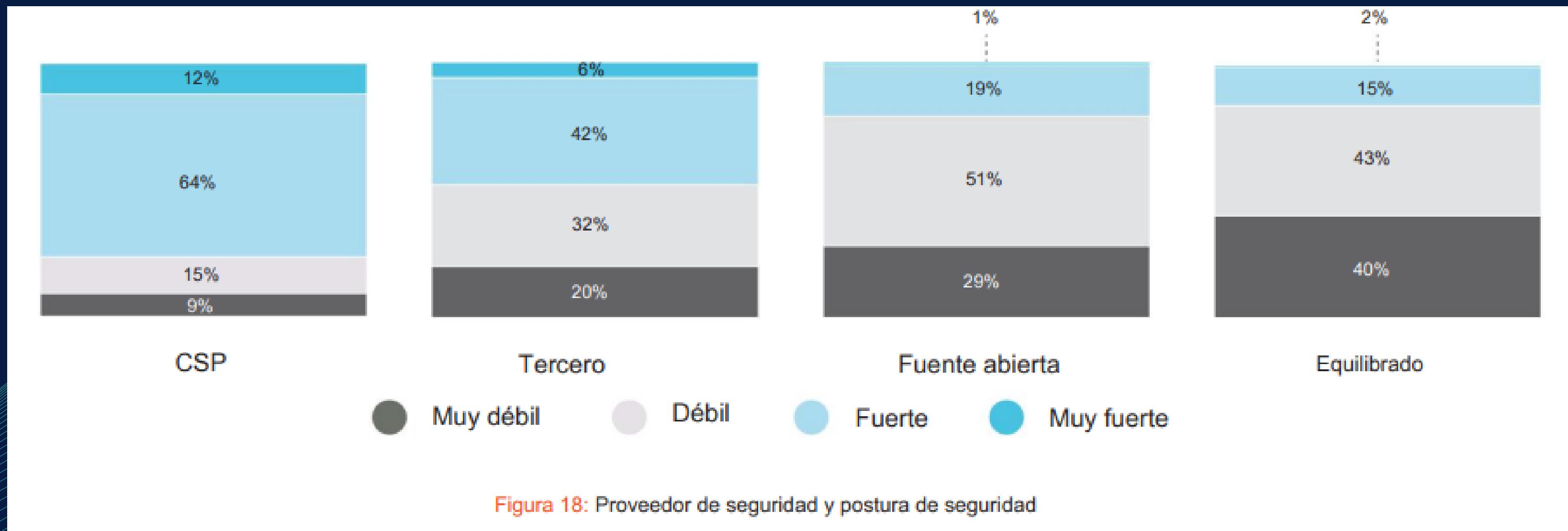
- Se evaluó la postura de seguridad (efectividad) y la fricción de seguridad (impacto en operaciones).
- El 55% tiene una postura de seguridad débil, sugiriendo áreas de mejora en actividades subyacentes.



Enfoques para una Postura de Seguridad Sólida:

Integración de DevSecOps y Automatización:

- Organizaciones que integran principios de DevSecOps tienen siete veces más probabilidades de tener una postura sólida.
- Automatización significativa de la seguridad también contribuye a resultados más sólidos.



Enfoques para una Postura de Seguridad Sólida:

Integración de DevSecOps y Automatización:

- Organizaciones que integran principios de DevSecOps tienen siete veces más probabilidades de tener una postura sólida.
- Automatización significativa de la seguridad también contribuye a resultados más sólidos.

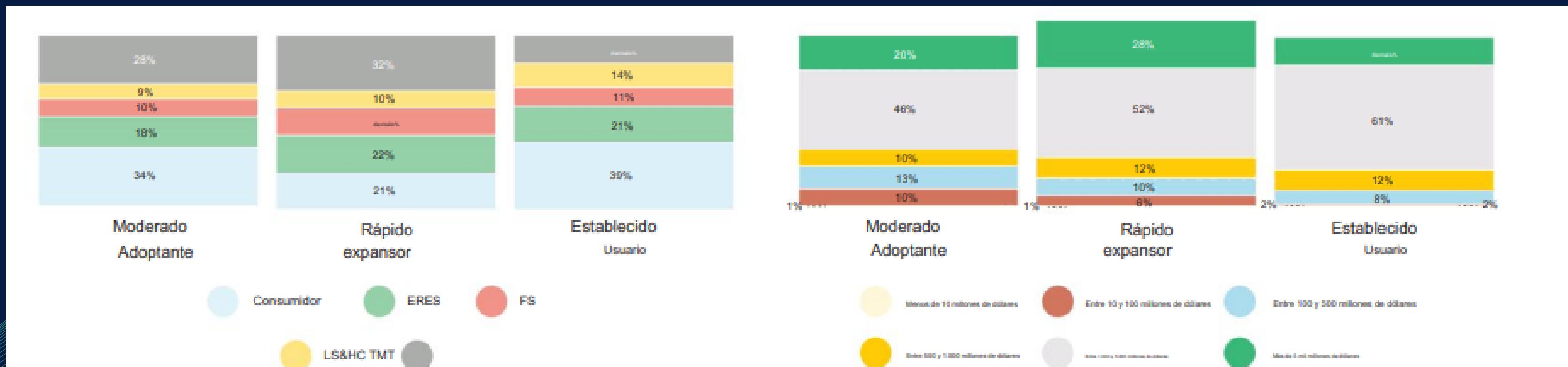


Figura 20: Grupos de adopción de la nube por industria (izquierda); Grupos de adopción de la nube por ingresos (derecha)

**La expansión
rápida en la
nube**

La Expansión Rápida de la Nube Produce Resultados Polarizantes

El grupo de Expansión Rápida se dividió en dos subgrupos distintos.

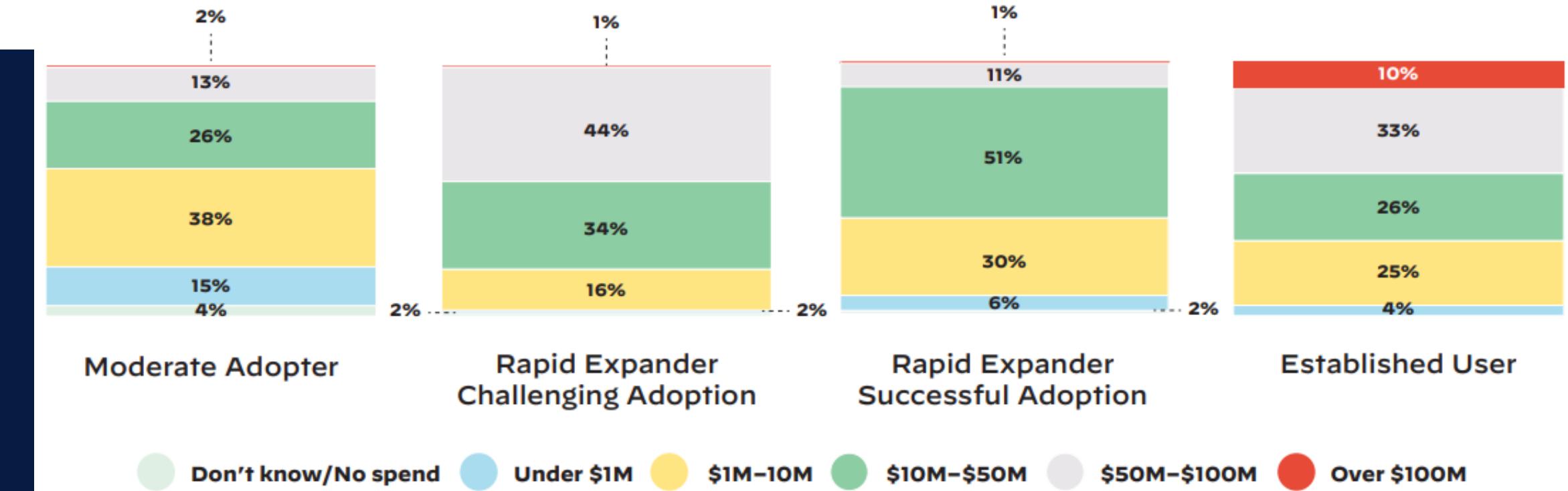
El 74% de los grupos de Expansión se apresuraron a aumentar con éxito su presencia en la nube.

El 26% restante de los Expansores Rápidos trasladó el 28% de las cargas de trabajo a la nube durante la pandemia.

| | 2020 | 2021 | Next Two Years |
|-------------------------------------|------|------|----------------|
| Moderate Adopter | 35% | 14% | +13% |
| Rapid Expander Challenging Adoption | 34% | 28% | -26% |
| Rapid Expander Successful Adoption | 24% | 35% | +12% |
| Rapid Expander | 61% | 13% | +10% |

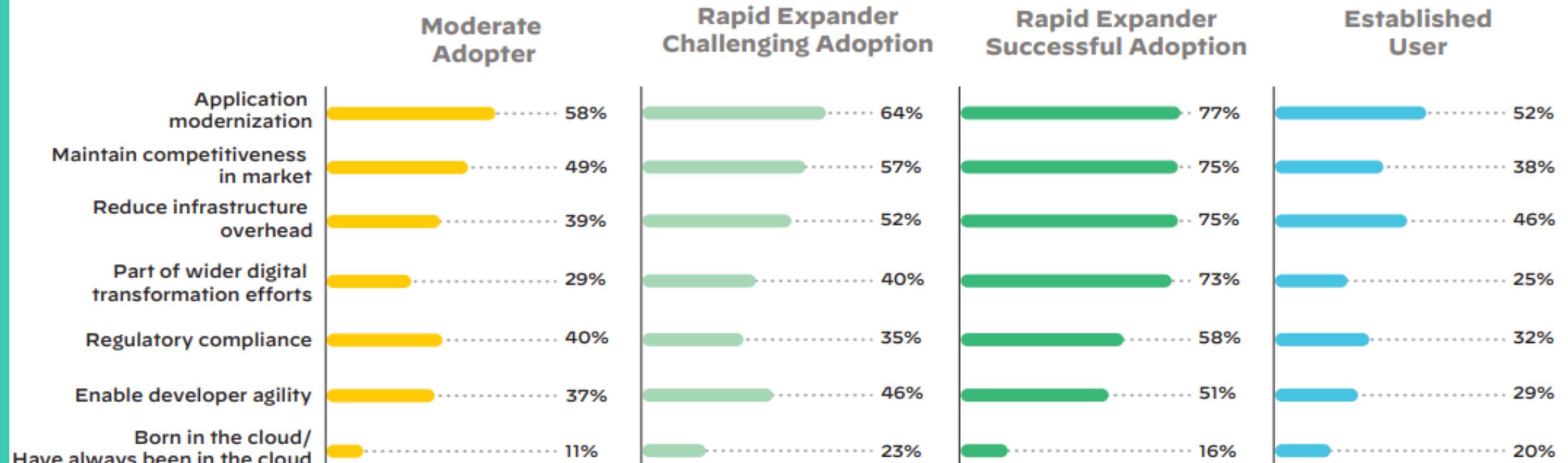
Crecimiento de la carga de trabajo en la nube para 2020–2021 y lo esperado para 2022–2023

- Los expansores rápidos tuvieron tanto éxitos como desafíos en sus esfuerzos de adopción en la nube.
- El 45% de los que enfrentaron desafíos gastaron más de \$50 millones en la nube en 2021.



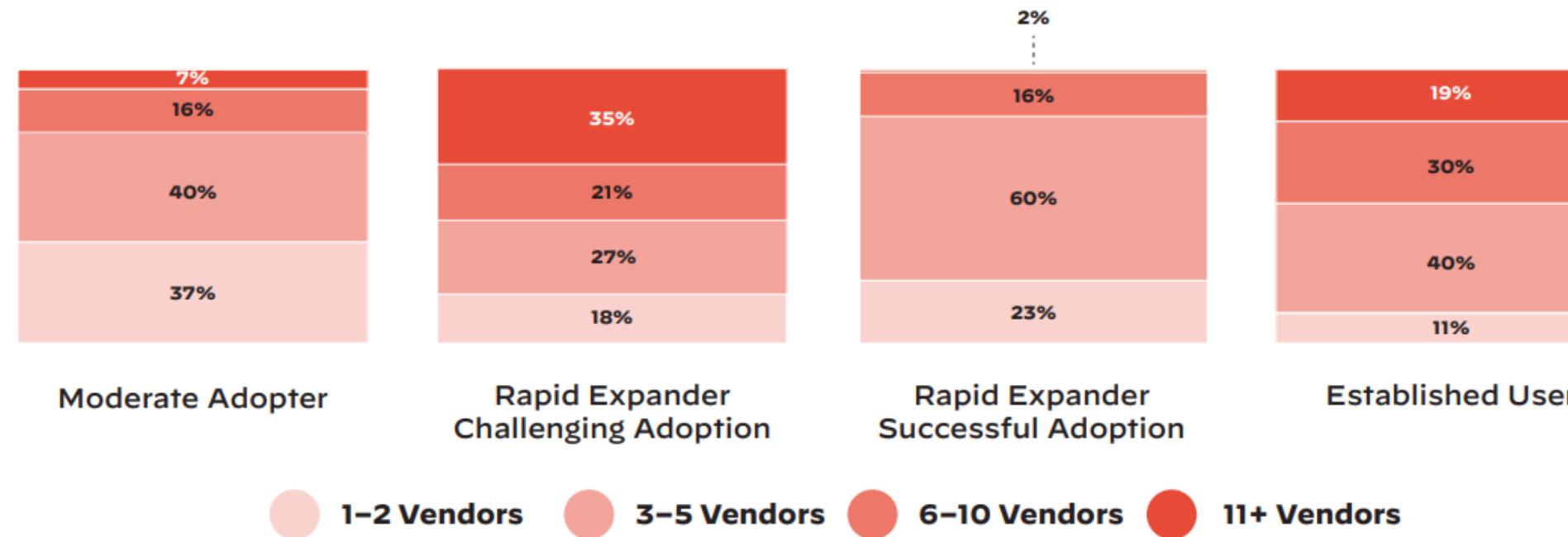
Razones para trasladar las cargas de trabajo a la nube

- Todos los grupos priorizaban metas a corto plazo, como modernizar aplicaciones y mantener la competitividad, en lugar de pensar de manera estratégica

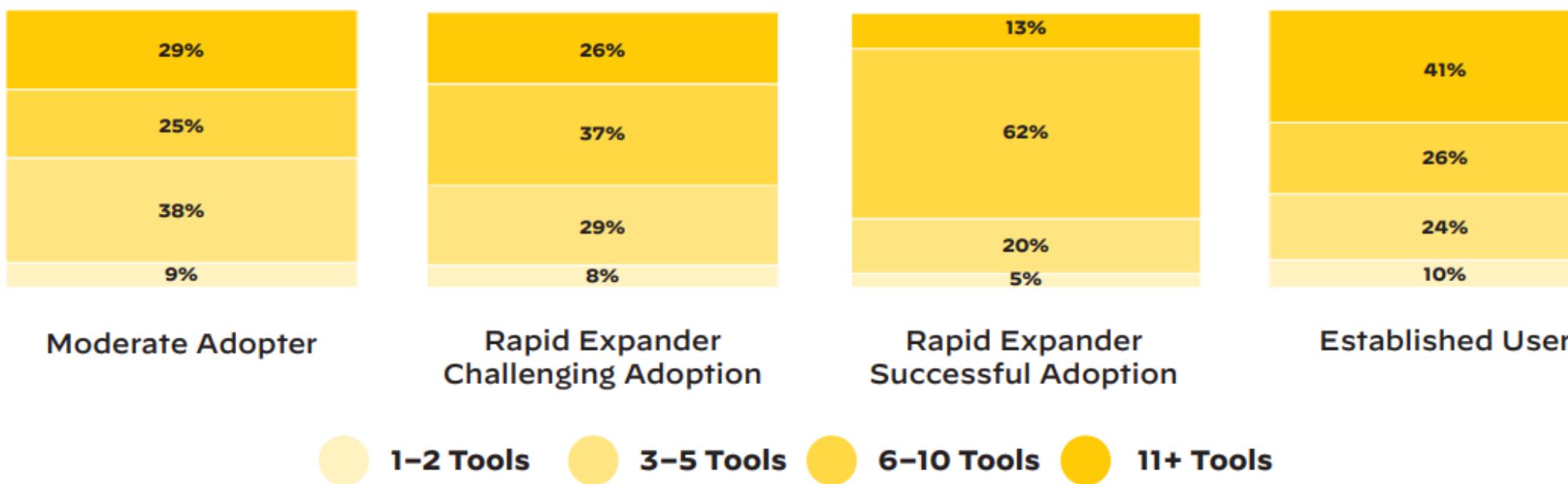


Niveles de gasto por grupo de adopción

El Rol de los Proveedores de Seguridad, Equipos y Herramientas



Número de proveedores de seguridad utilizados



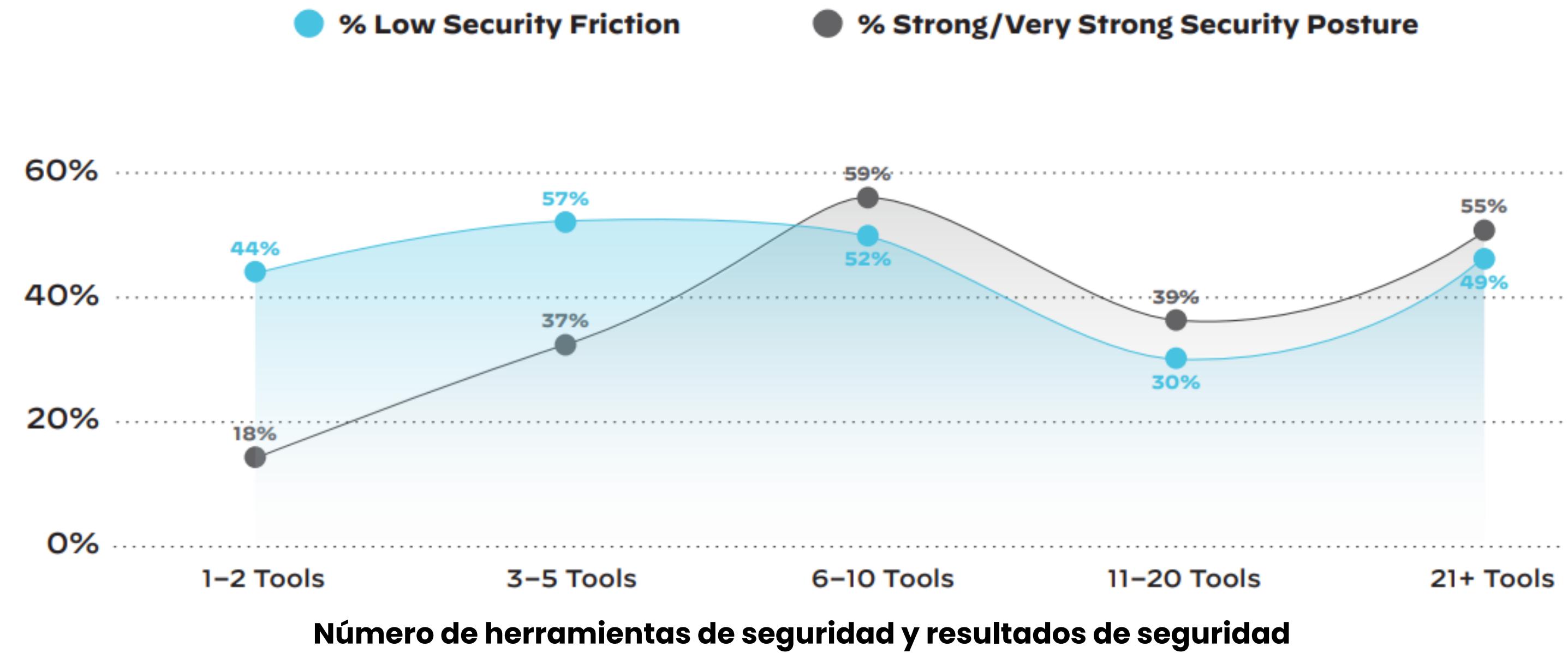
Número de herramientas utilizadas, independientemente del proveedor

Los dos grupos de Expansión Rápida optaron por estrategias diferentes al asociarse con proveedores de seguridad.

El 83% de los grupos con éxito utilizó cinco o menos proveedores.

Los entornos de nube más grandes pueden necesitar más herramientas, y diferentes equipos pueden preferir conjuntos distintos.

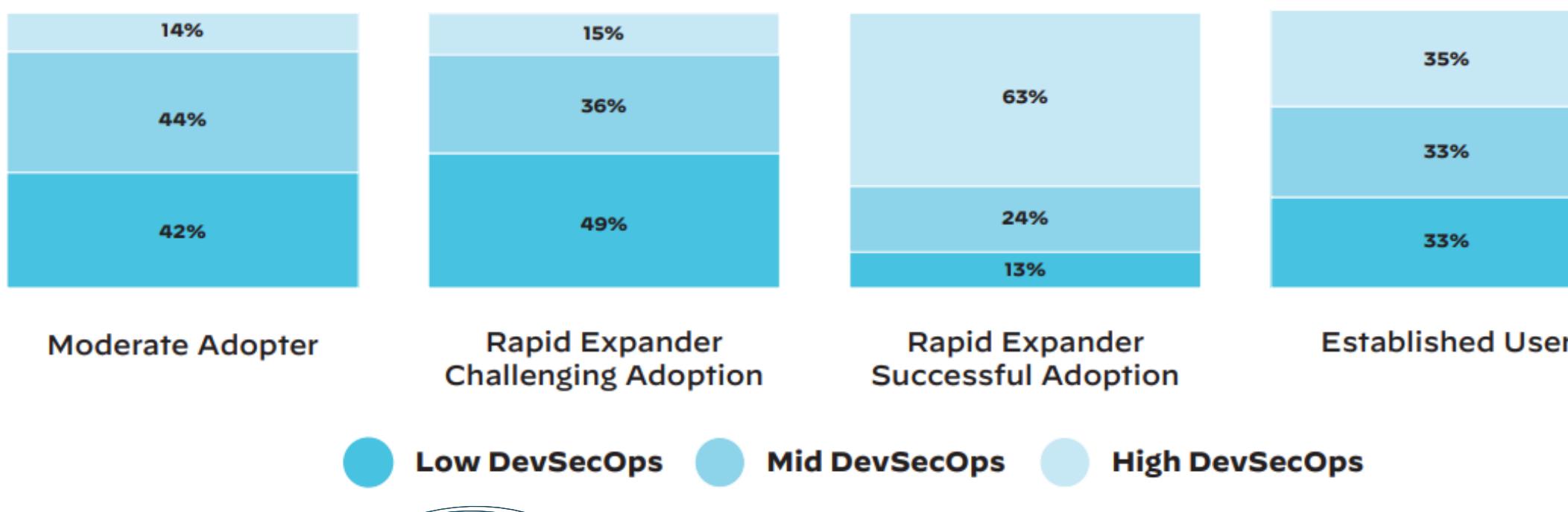
Los entornos de nube más grandes pueden necesitar más herramientas, y diferentes equipos pueden preferir conjuntos distintos.



Las empresas que aprovechan menos de cinco herramientas de seguridad luchan por ofrecer una postura de seguridad fuerte.

La integración de herramientas de seguridad es crucial.

Adopción Grupal de la Seguridad de Clase Mundial

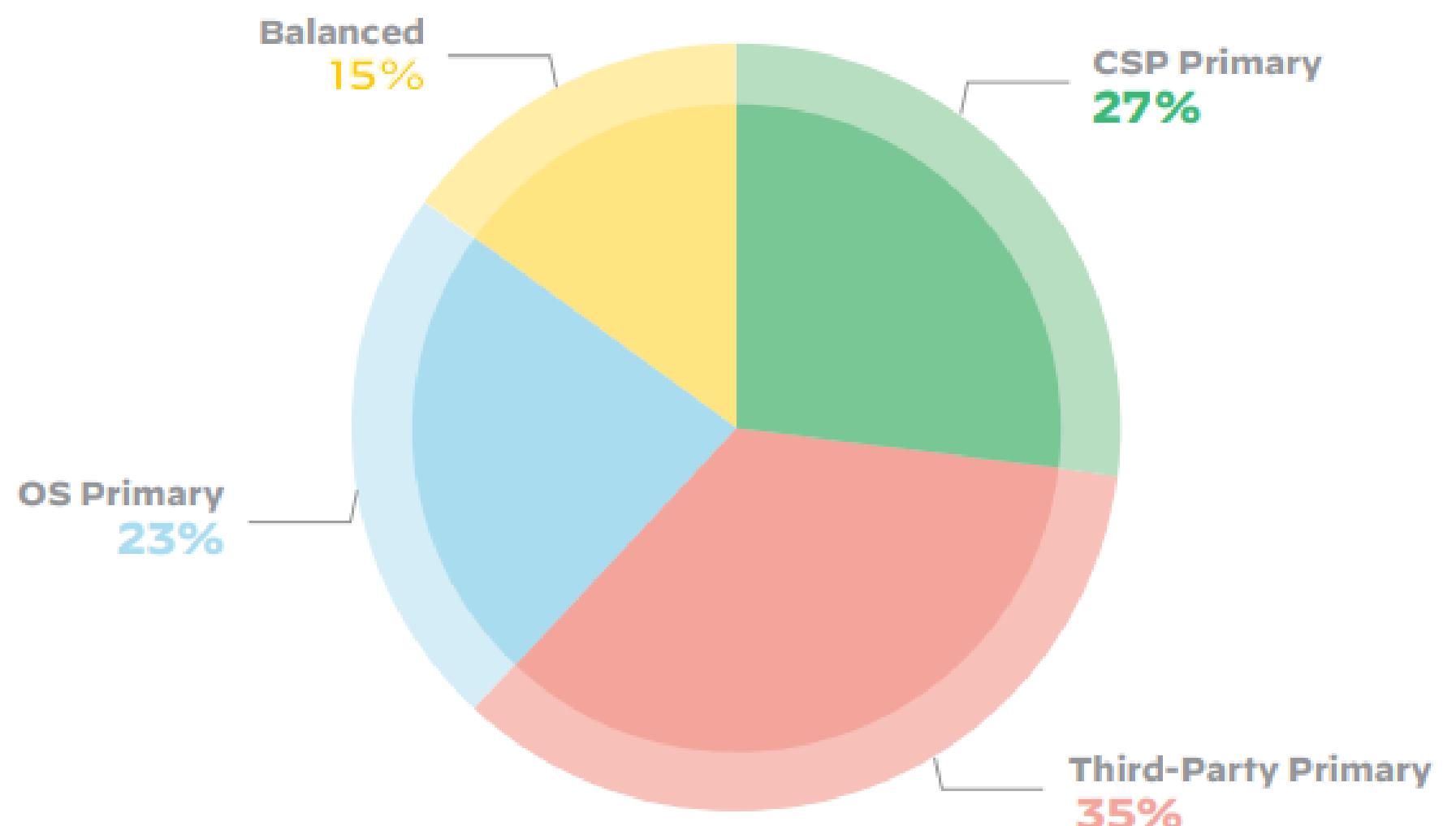


Nivel de integración de DevSecOps en el ciclo de vida de la aplicación

El 63% de los Expansores Rápidos que expandieron con éxito su adopción en la nube también incorporaron los principios de DevSecOps.

Los Expansores Rápidos que tuvieron éxito muestran la postura de seguridad más sólida, con un 81% clasificado como fuerte o muy fuerte.

Adopción Grupal de la Seguridad de Clase Mundial



1 Un gasto elevado en la nube no garantiza una adopción exitosa.

2 Integrar la adopción en la nube es esencial para el éxito.

3 La consolidación de proveedores de seguridad con diversas herramientas impulsa con éxito la adopción en la nube.

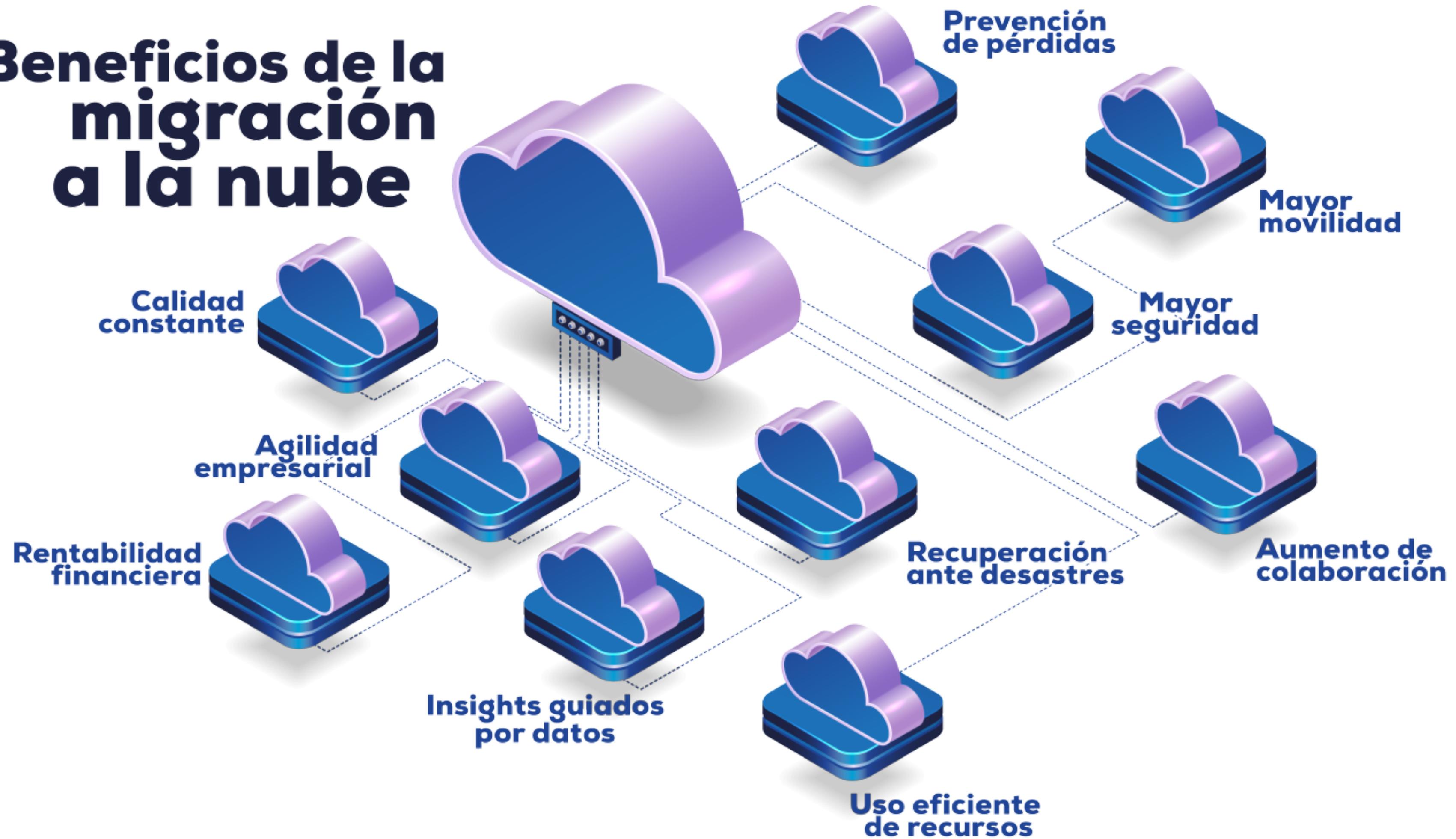
4 Equipos de seguridad más grandes no aseguran una organización más segura.

5 La integración de DevSecOps son componentes necesarios.

6 Los proveedores de seguridad ofrecen la mayor probabilidad de una adopción exitosa y segura de la nube.

Panorama en la Nube en 2022

Beneficios de la migración a la nube



Frecuencia de Ataques en la Nube

En el proceso de adopción de la nube, la configuración y provisión se priorizó sobre la seguridad.

Se ha reflejado en un importante aumento de amenazas y filtración de datos en la nube.

92%

de organizaciones hospedan parte de su entorno de TI en la Nube

79%

de las empresas han experimentado al menos una filtración de datos en la nube en los últimos 18 meses.

24%

de las empresas han informado de 10 o más filtración de datos en la nube en los últimos 18 meses.

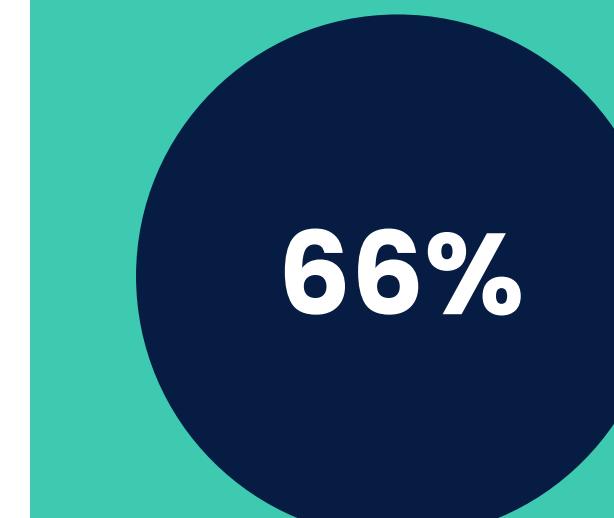
Desafíos de la Seguridad en la Nube

De los 5 principales desafíos asociados con las nubes publicas el mas reportado se asocia a controlar los costos en la nube



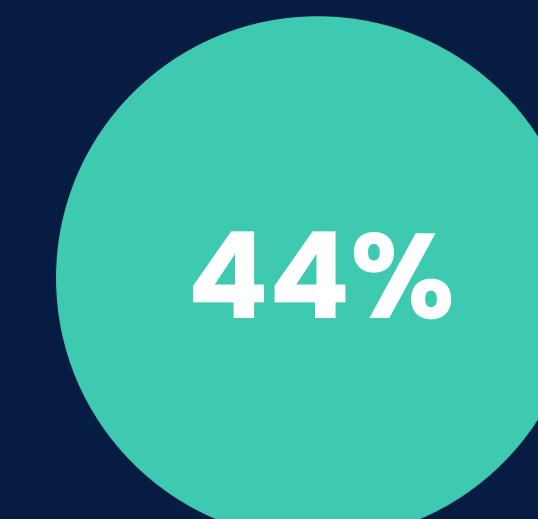
69%

Pérdida y Fuga de Datos



66%

Privacidad y Confidencialidad de Datos



44%

Exposición Accidental de Credenciales

¿Cómo se están Preparando Actualmente las Empresas?

93% de las empresas mencionan la preocupación acerca de errores humanos que pueden provocar la exposición accidental de datos

22% de las organizaciones aún evalúan su postura de seguridad manualmente



Solo una de cada cinco empresas evalúa su postura de seguridad en tiempo real.



Una de cada cinco empresas realiza evaluaciones semanales de su postura de seguridad.



El 58% de todas las empresas evalúan su postura de seguridad solo una vez al mes o con menos frecuencia.

Amenazas comunes a la seguridad en la nube

Amenazas en la nube

1. Configuración incorrecta y error humano

- Retrasa detección de violaciones de seguridad.
- 34% de violaciones de identidad en cuentas privilegiadas. Solo el 38% de organizaciones usan autenticación multifactor.
- 90% de identidades en la nube utilizan menos del 5% de sus permisos otorgados

2. Ataques de toma de control de cuentas

- Phishing constituye más del 90% de violaciones de datos según CISCO (2021).
- Redes de entrega de contenido permiten alojar archivos maliciosos con facilidad.
- Bloquear dominios de phishing es difícil sin eliminar todo el contenido, incluso el legítimo.

3. Ransomware

- 59% de incidentes de ransomware donde los datos se cifran son en la nube pública
- Los datos cifrados se ocultan en servicios como: Google Drive, Amazon S3 o Mega.nz
- Esto dificulta la localización de datos.

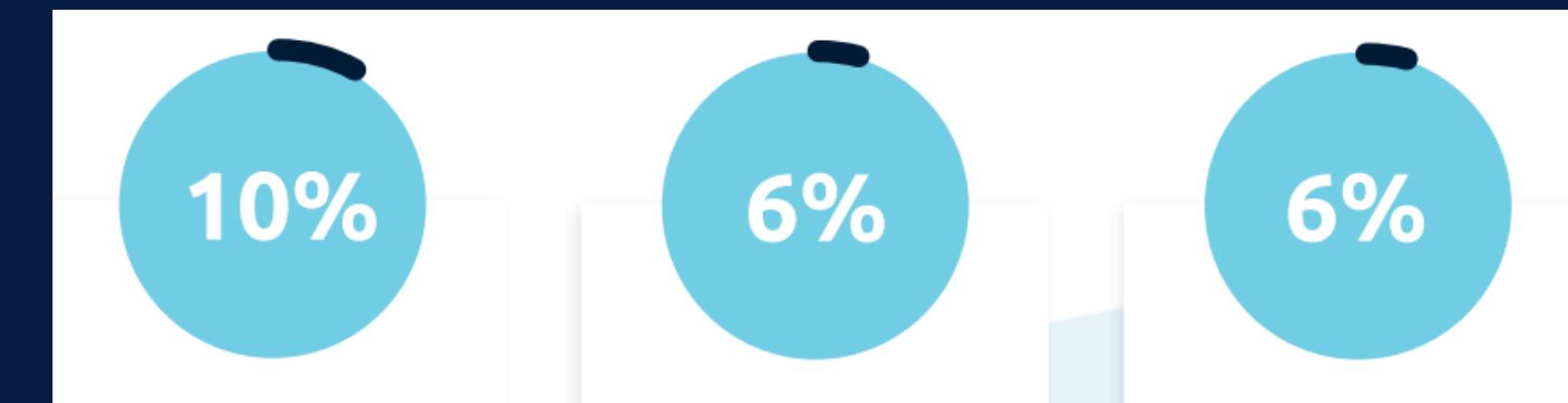
Victimas de ataques en la nube

- Organizaciones de cualquier tipo suelen ser blanco de ataques.
- La principal preocupación de seguridad en la nube para las empresas es la privacidad y protección de datos
- Dentro del volumen de ataques en la nube se encuentra la siguiente estadística.



Empresas
tecnológicas

Organizaciones de
salud



Agencias
Gubernamentales

Compañías
financieras

Negocios de
hostelería

Microsoft Azure Sentinel

- Es una solución de Gestión de Información y Eventos de Seguridad (SIEM) y de Orquestación, Automatización y Respuesta de Seguridad (SOAR)
- Ofrece análisis de seguridad inteligentes e inteligencia de amenazas en toda la organización
- Proporciona una vista panorámica única y completa de la seguridad de tu negocio
- Su funcionamiento en la nube elimina los gastos de hardware y garantiza una implementación eficiente



Características de Microsoft Azure Sentinel

Acceso

Investigación de amenazas con inteligencia artificial

Integración de aplicaciones

Respuesta rápida ante incidentes

Amigable con entornos híbridos

Respuestas personalizadas

Conclusiones

- La seguridad en la nube evoluciona con una consolidación de proveedores y herramientas, destacando la importancia de una postura sólida y baja fricción.
- La integración de DevSecOps, automatización y decisiones estratégicas en la selección de herramientas son fundamentales para el éxito.
- La identificación y aprendizaje de grupos en la nube pueden proporcionar información valiosa para la planificación futura.
- A pesar de las preocupaciones y desafíos, muchas empresas no están fortaleciendo suficientemente su postura de seguridad. Sin embargo, la gestión adecuada y las provisiones de seguridad pueden mitigar los riesgos.
- A lo largo de la rápida evolución en las estrategias y recursos empresariales, las organizaciones han experimentado en su mayoría éxitos al expandirse hacia la nube durante este período de transformación.

Muchas Gracias

