Global Data Protection Index: edición especial 2024

Conclusiones clave: octubre de 2023

VansonBourne

DELL Technologies

Enfoque de las conclusiones clave

1
El panorama de riesgos de la protección de datos

2
La creciente amenaza de ataques cibernéticos

3
El uso de las múltiples nubes

4
Protección del entorno de nube

Cinco puntos clave

Los ataques cibernéticos continúan en aumento

El costo de los ataques cibernéticos está aumentando

Las pólizas de seguros no cubren lo suficiente del costo de los ataques

Un mayor uso de IA generativa podría dar lugar a datos de mayor valor

Esto genera que los ataques cibernéticos supongan mayores riesgos e impacto financiero

DELL Technologies

¿A quiénes entrevistamos?

Se entrevistó a 1500 tomadores de decisiones de TI y seguridad de TI en septiembre y octubre de 2023

Organizaciones de una amplia variedad de industrias públicas y privadas

Organizaciones que tienen más de 250 empleados

4 regiones:

América (300)
EMEA (675)
APJ (375)
China (150)

1. El panorama de riesgos de la protección de datos

La preocupación por las medidas de protección de datos es generalizada y, ante la falta de confianza, las organizaciones se encuentran en una posición vulnerable.

Un 60 %

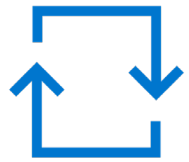
no está muy seguro de que su organización esté **cumpliendo con los objetivos de nivel de servicio de respaldo y recuperación (SLO)**

Un 79 %

está **preocupado** por la posibilidad de **sufrir un evento disruptivo** en los próximos doce meses

Un 75 %

está **preocupado** de que las medidas de protección de datos existentes en su organización **no sean suficientes para hacer frente a amenazas de malware y ransomware**

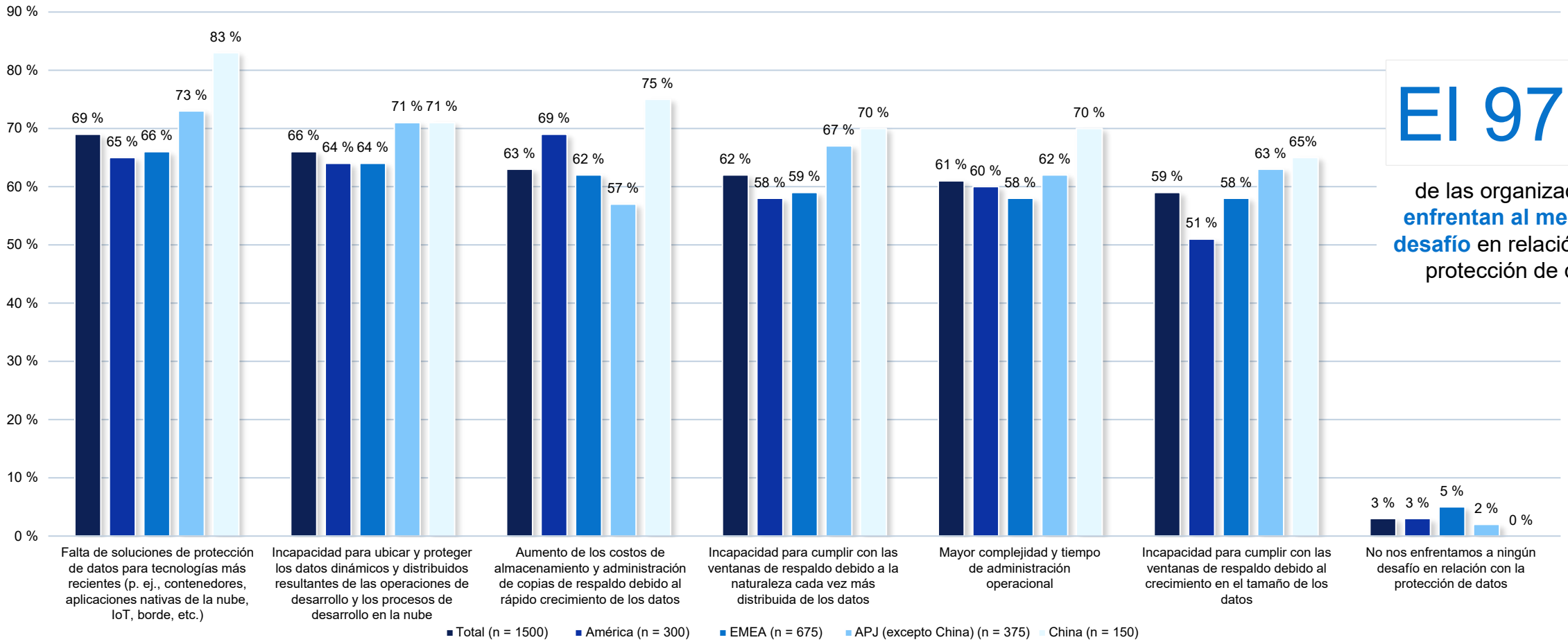


Un 65 %

no está muy seguro de que su organización pueda **recuperar completamente los sistemas o los datos de todas las plataformas** en caso de un incidente de pérdida de datos

Además de las preocupaciones por la protección de datos, muchas organizaciones enfrentan desafíos

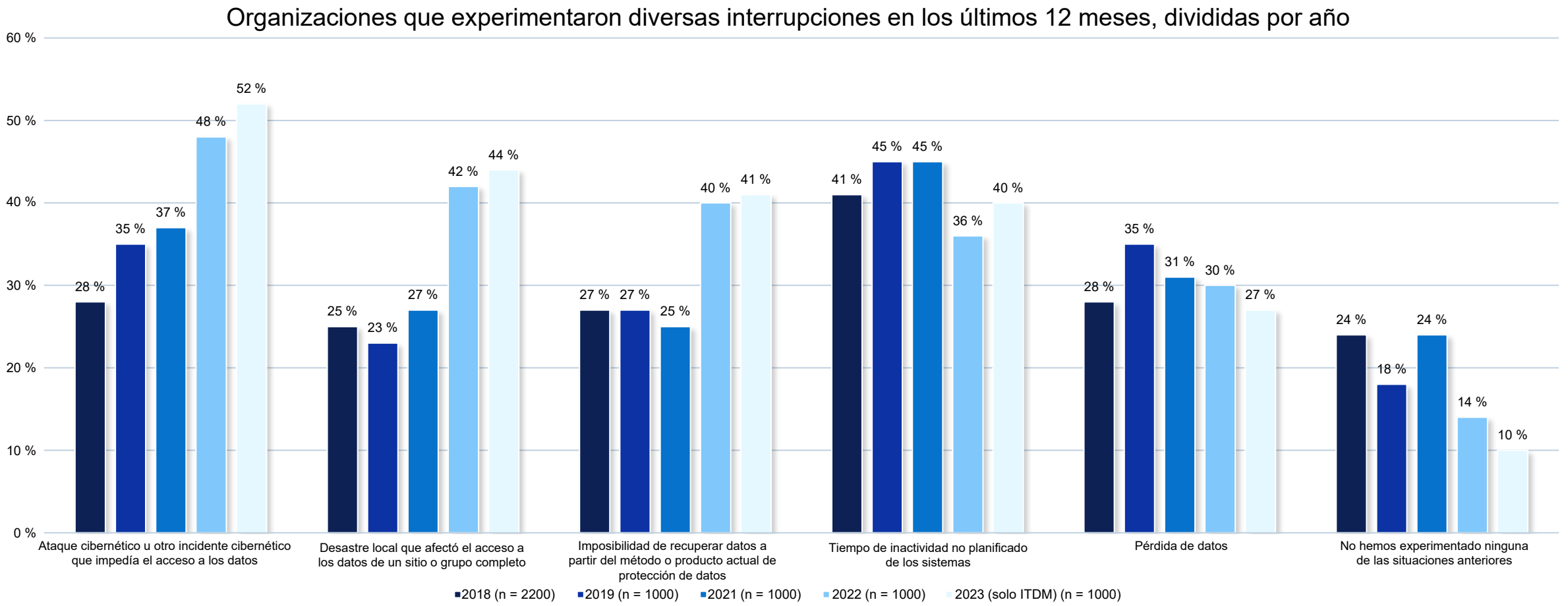
Clasificado entre los 5 principales: desafíos en relación con la protección de datos, dividido por región



El 97 %

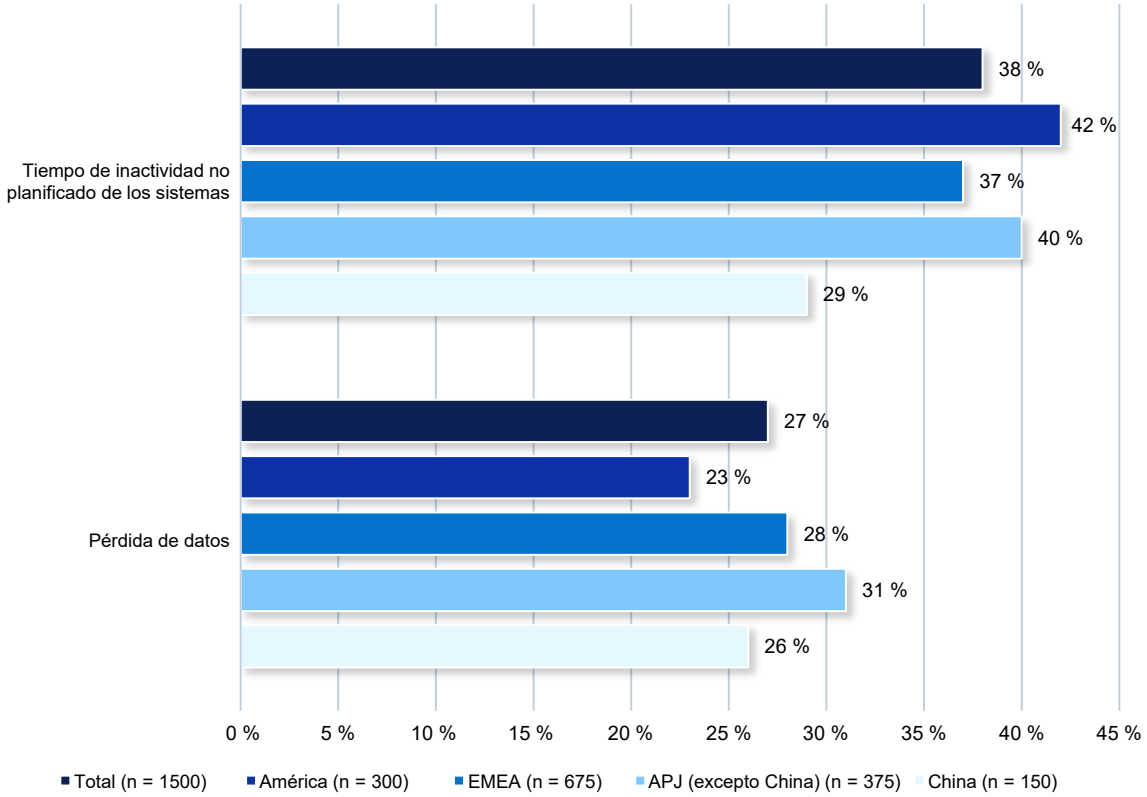
de las organizaciones **enfrentan al menos un desafío** en relación con la protección de datos

En los últimos 12 meses, las organizaciones enfrentaron interrupciones significativas, con ataques cibernéticos que suponen una amenaza cada vez mayor y más presente



La pérdida de datos no solo contribuyó a la interrupción, sino que también afectó el balance final

Porcentaje de organizaciones que experimentaron tiempo de inactividad no planificado de los sistemas o pérdida de datos en los últimos 12 meses, dividido por región



En los últimos 12 meses:

26 horas

de tiempo de inactividad no planificado de los sistemas, experimentado en promedio

2,45 TB

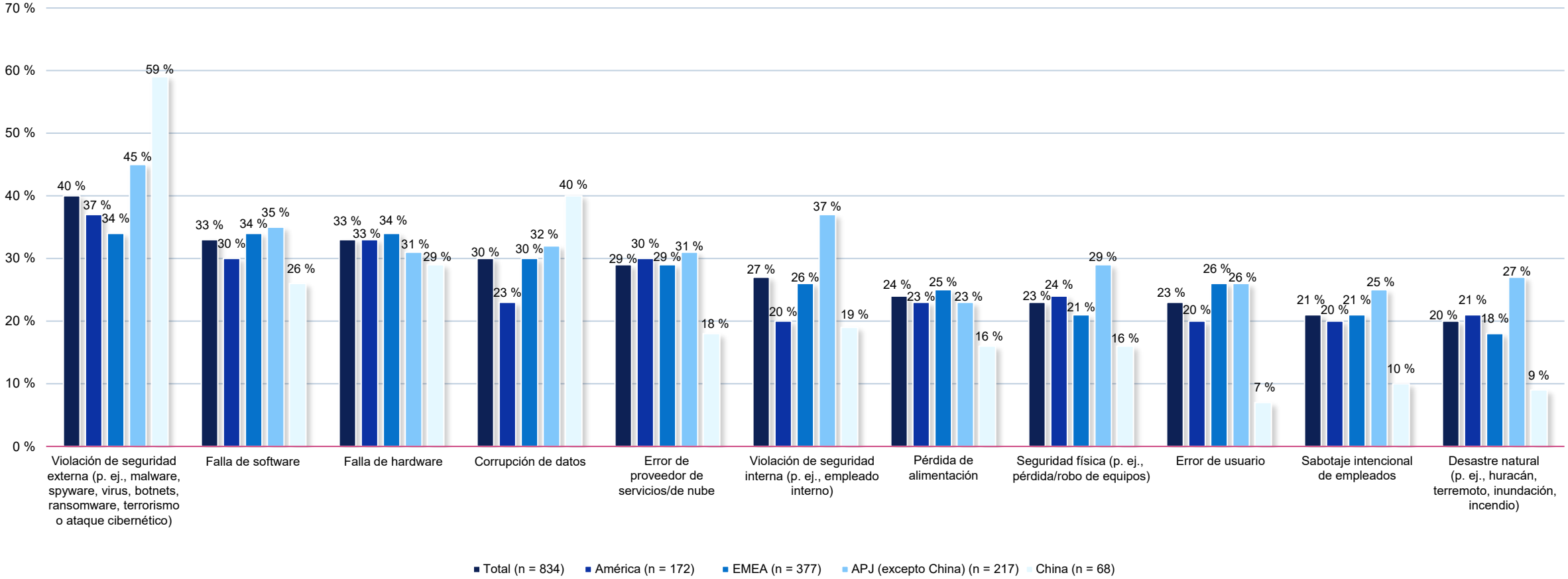
es el volumen de información perdido, en promedio

$2,61

millones, es el promedio del **costo de la pérdida de datos**

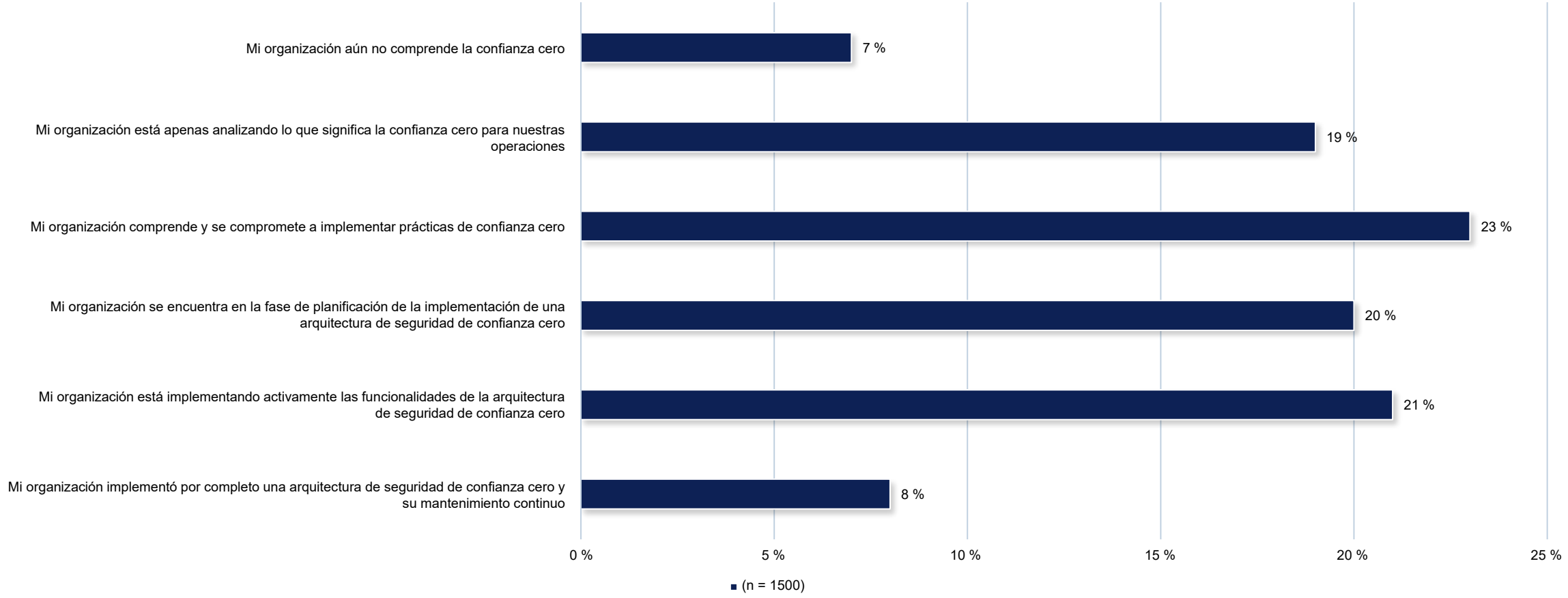
Las amenazas de seguridad externas son las causas más comunes de la pérdida de datos o el tiempo de inactividad no planificado de los sistemas durante los últimos 12 meses

Causa de la pérdida de datos o el tiempo de inactividad en los últimos 12 meses



A pesar de los desafíos y las preocupaciones por la protección de datos, pocos implementaron por completo la seguridad de confianza cero

El viaje de las organizaciones hacia la implementación de la seguridad de confianza cero

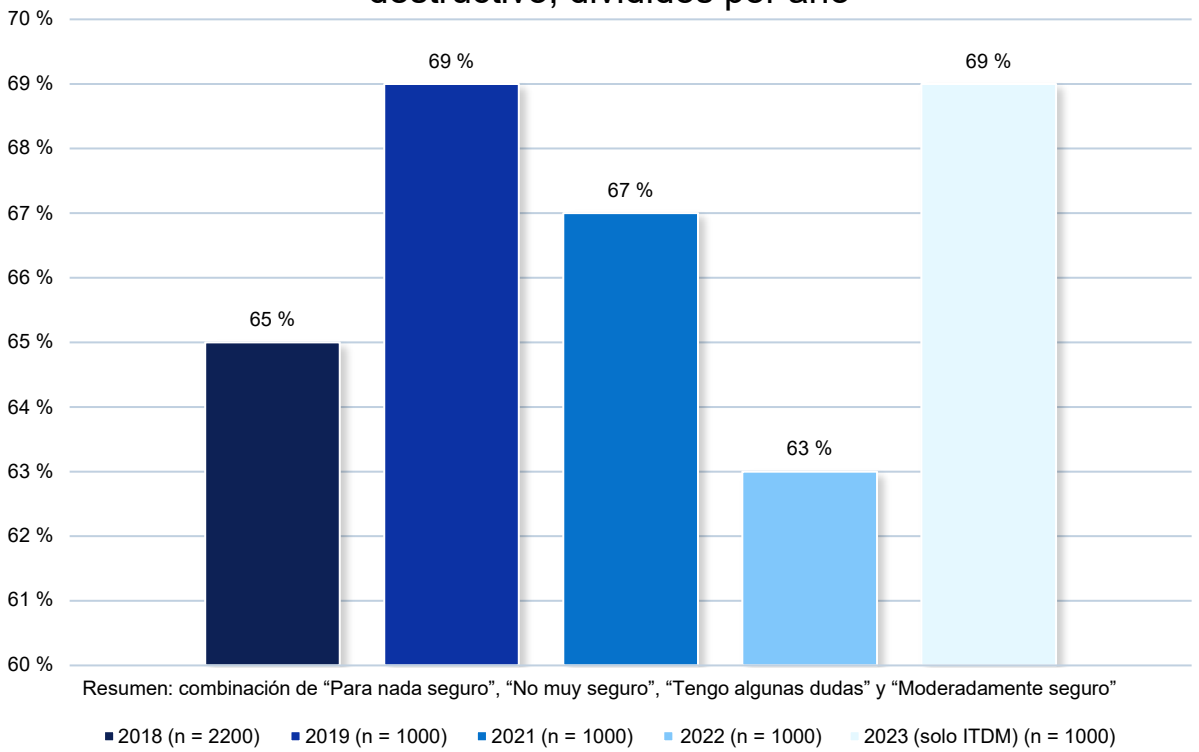


Filtro: división de datos: región = total

2. La creciente amenaza de ataques cibernéticos

La preocupación por las medidas de protección de datos es generalizada y, ante la falta de confianza, las organizaciones se encuentran en una posición vulnerable

No "muy seguros" de que todos los datos críticos de la empresa se puedan recuperar de forma fiable en caso de un ataque cibernético destructivo, divididos por año



Un 81 %

está de acuerdo en que su organización está **más expuesta a la pérdida de datos debido a amenazas cibernéticas** con el aumento de los empleados que trabajan desde el hogar

Un 74 %

les **preocupa** que sus datos de respaldo puedan **infectarse o dañarse debido a ataques de ransomware**

Además del riesgo, hay un exceso de confianza erróneo en torno a las consecuencias de un ataque de ransomware

72 %

afirma que su trabajo y los empleados de su organización **no se verán afectados por un ataque de ransomware**

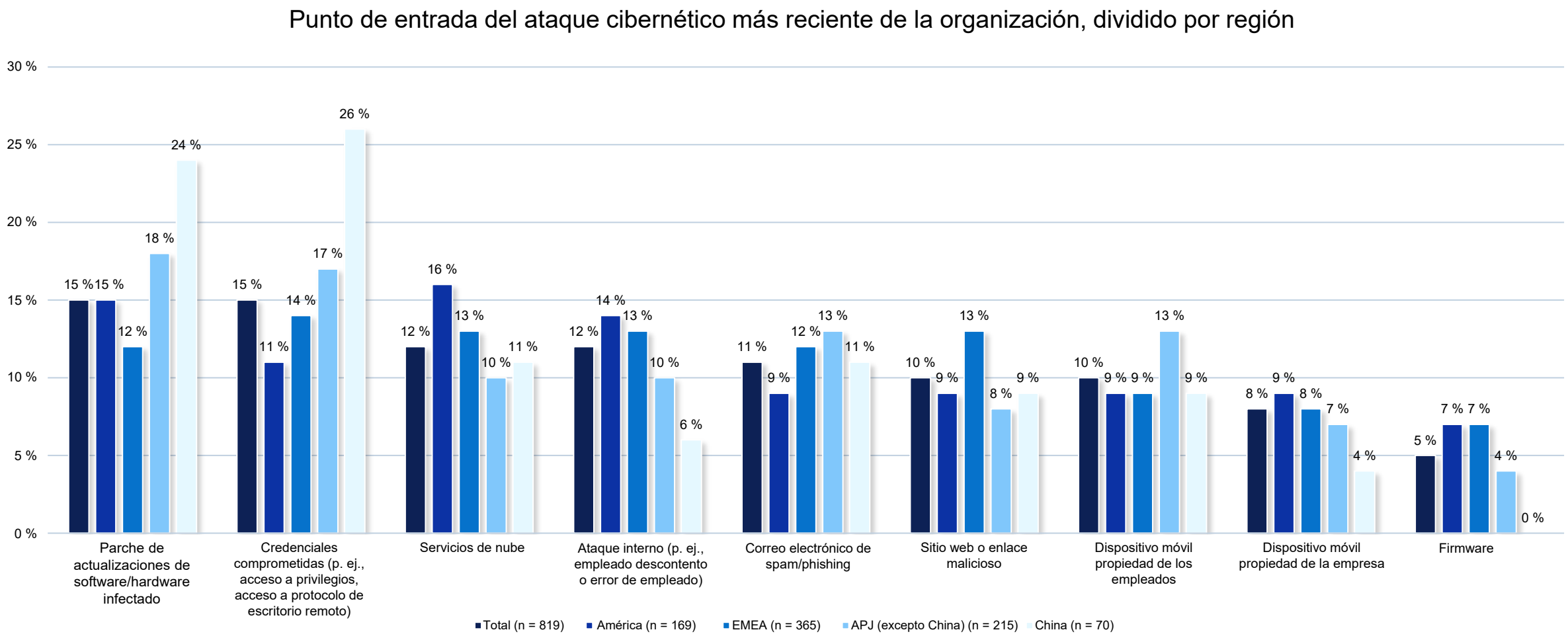
74 %

afirma que si su organización sufre un ataque de ransomware, recuperará **todos los datos** para reanudar el negocio **si pagan el rescate**

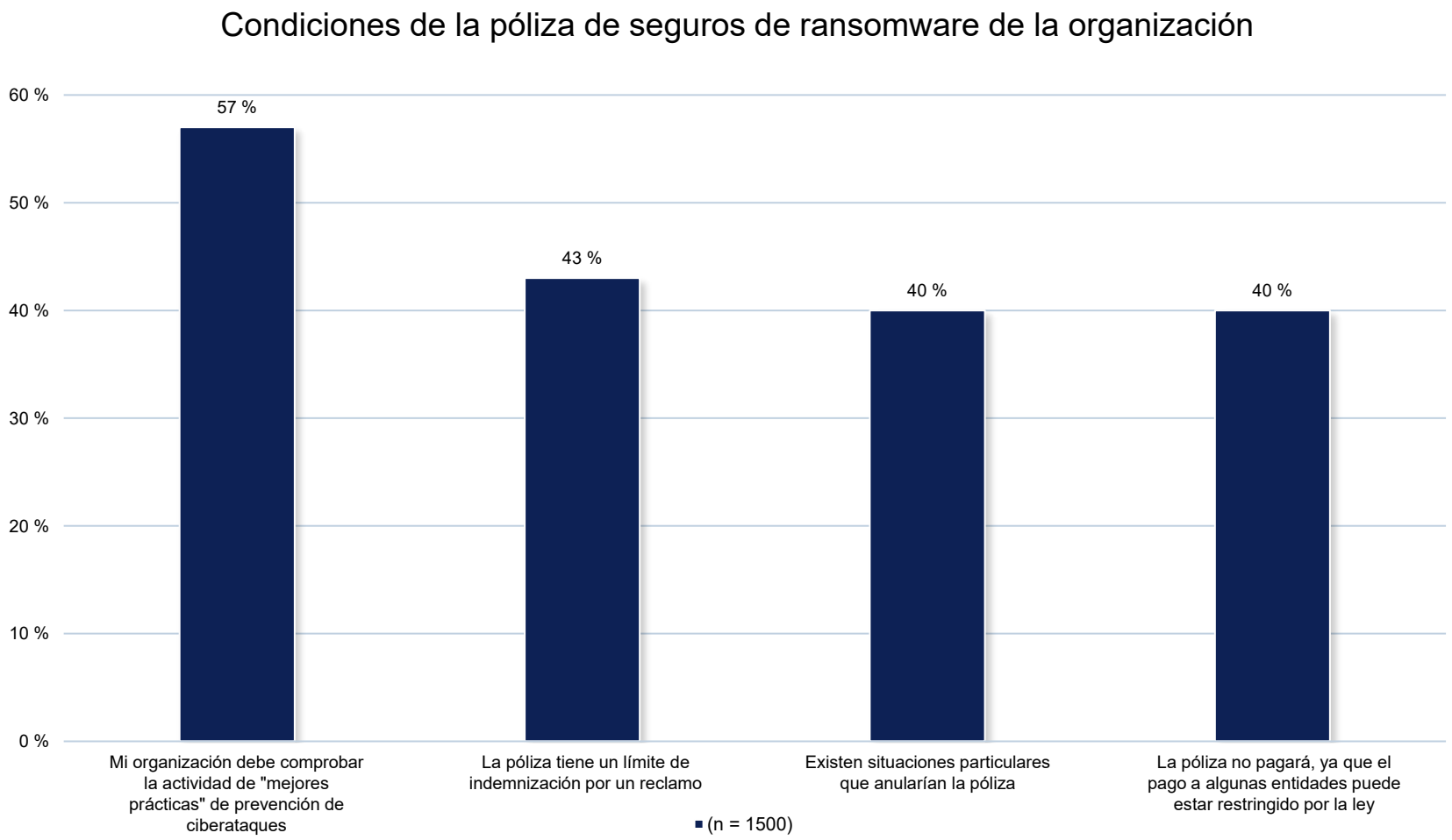
66 %

afirma que si su organización sufre un ataque de ransomware, una vez que pague el rescate **no será atacada nuevamente**

Los delincuentes cibernéticos apuntan a varios puntos de entrada, con más probabilidades de ataques provenientes de fuentes externas



Las pólizas de seguro de ransomware son comunes entre las organizaciones, pero se encuentran muy condicionadas

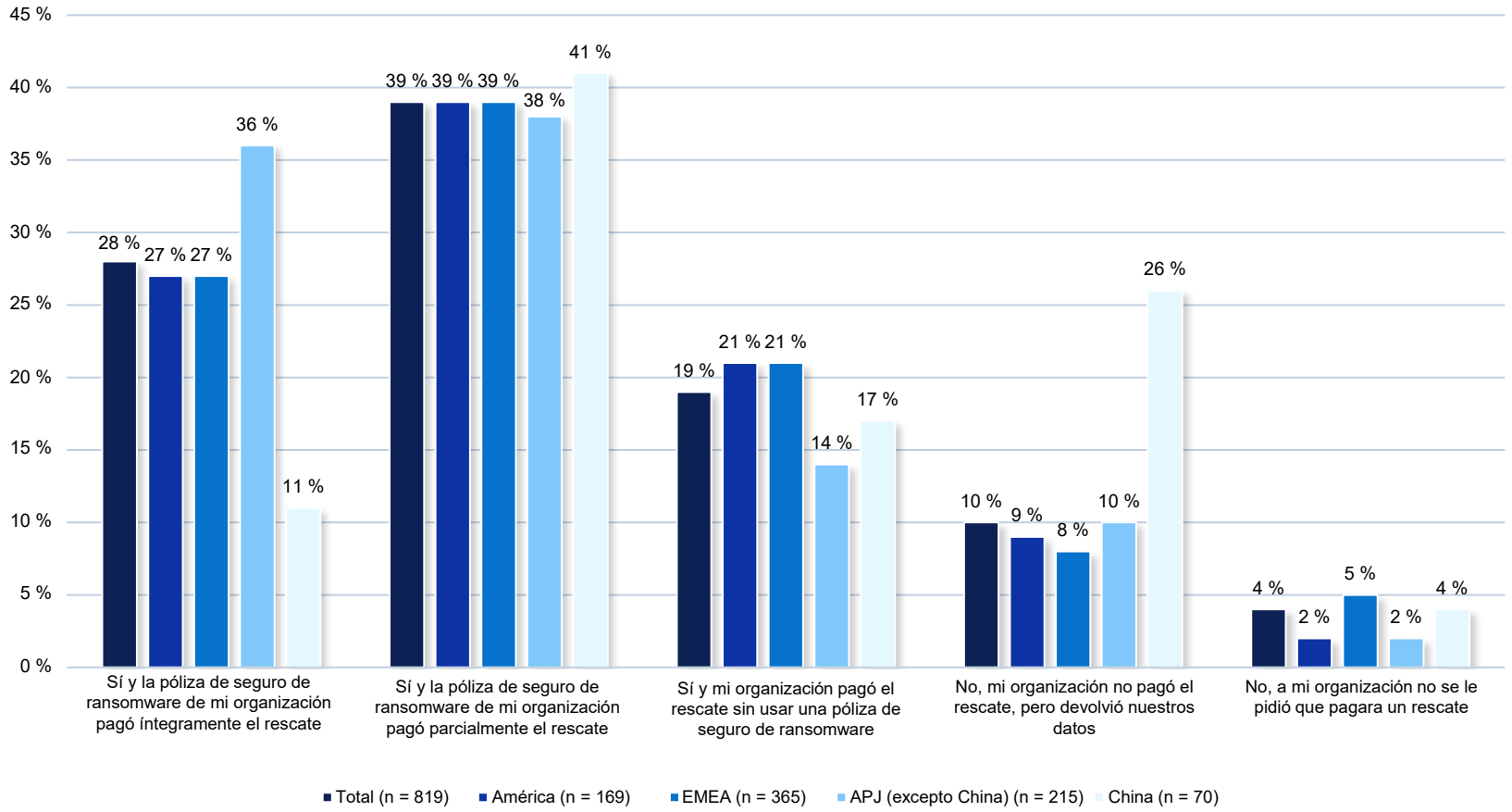


El 93 %

de las organizaciones **tienen una póliza de ransomware**

A pesar de que muchas tienen pólizas de ransomware implementadas, las organizaciones aún se encuentran vulnerables desde el punto de vista financiero

"¿Se pagó un rescate para obtener acceso a los datos de su organización?", dividido por región

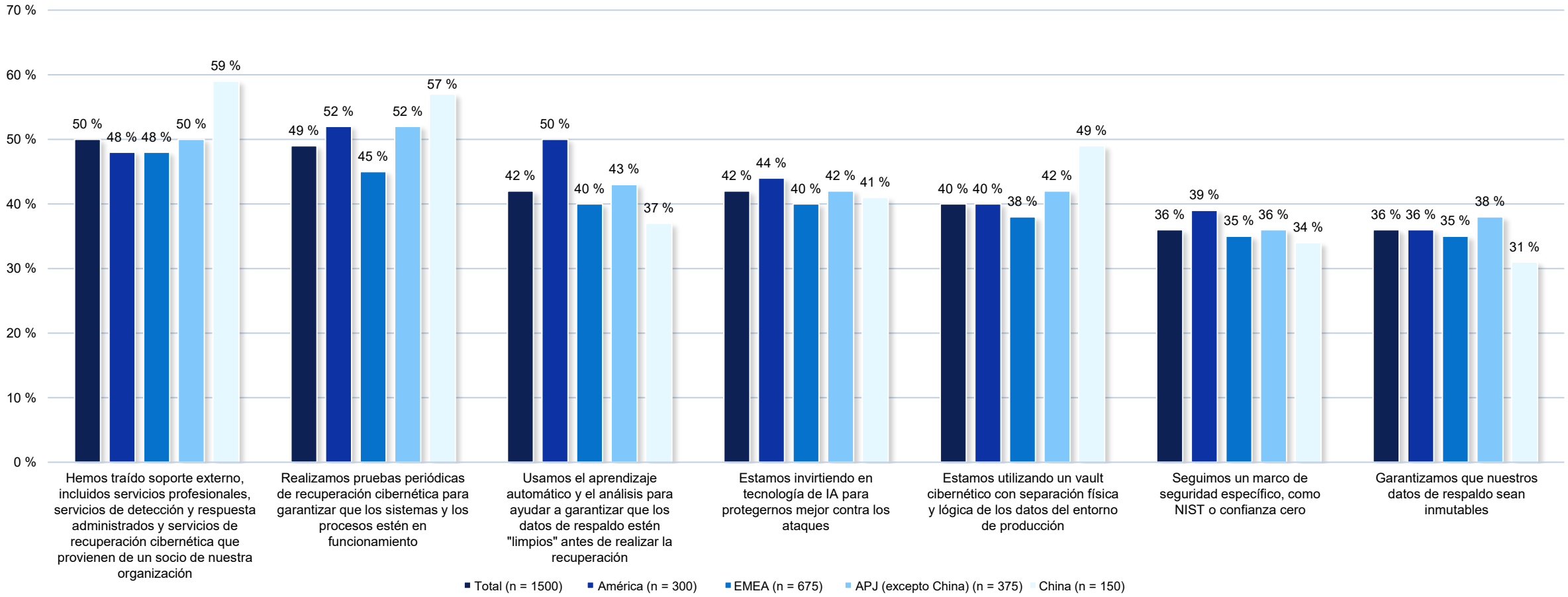


$1,92

millones: el costo promedio para las organizaciones en los últimos 12 meses que provocaron los **ataques cibernéticos y otros incidentes relacionados con la ciberseguridad**

Afortunadamente, las organizaciones están tomando medidas para aumentar su resiliencia cibernética

Medidas que las organizaciones están tomando para mejorar su resiliencia cibernética, dividida por región

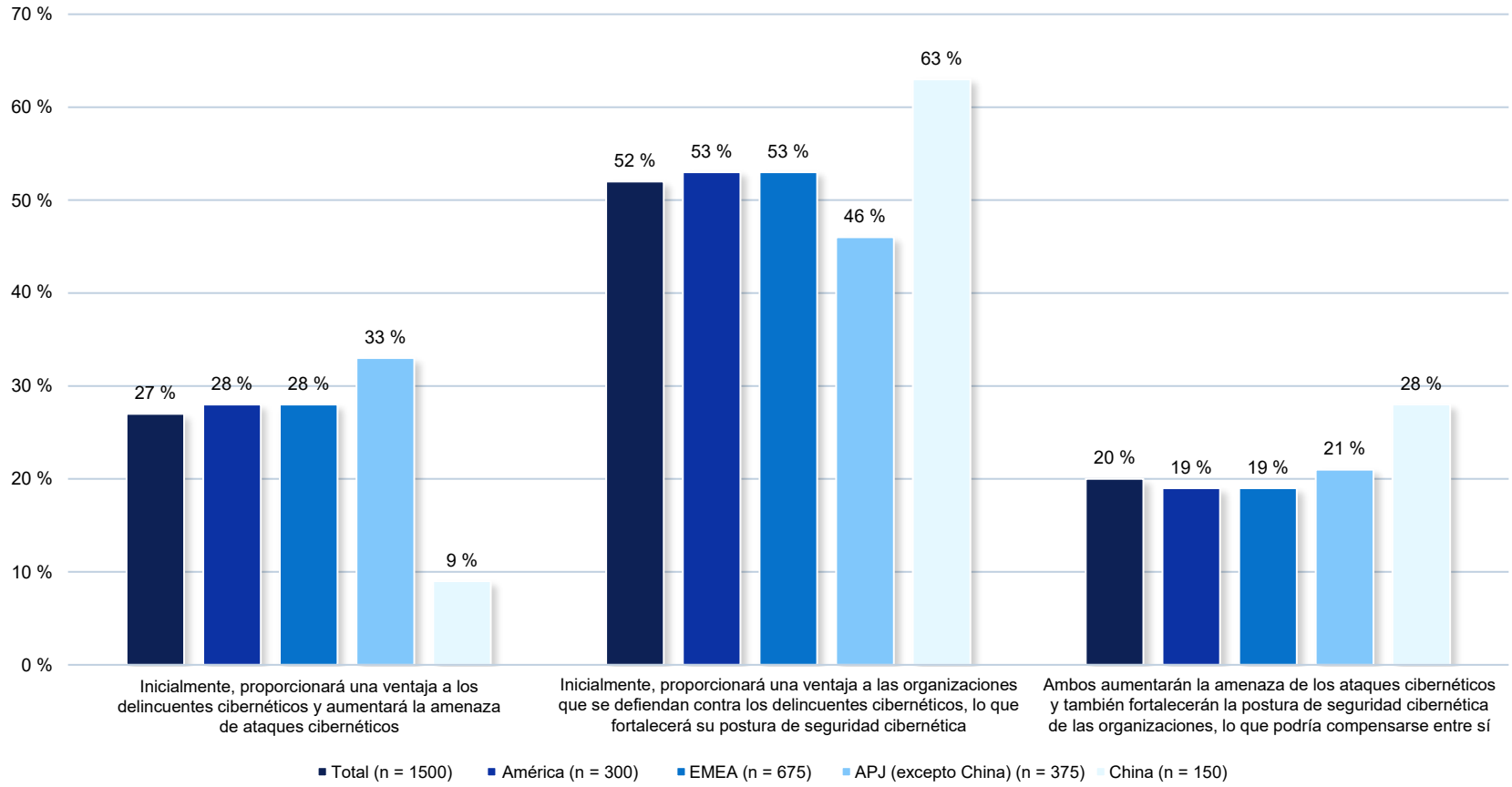


Sin embargo, no todos creen que la IA generativa beneficiará su resiliencia cibernética

Un 81 %

afirma que las tecnologías emergentes (como la inteligencia artificial, IoT y el borde) **suponen un riesgo para la protección de datos**

Impacto de la IA generativa en las amenazas cibernéticas y la seguridad de los datos, dividida por región



De hecho, con organizaciones que ya están preocupadas por la protección de datos, muchos creen que la IA generativa creará nuevos desafíos

Un 88 %

afirma que la IA generativa creará grandes volúmenes de datos nuevos **que deberán protegerse y asegurarse**

Un 88 %

afirma que la IA generativa aumentará el valor de ciertos tipos de datos, lo que requeriría **niveles de servicio de protección de datos más altos**

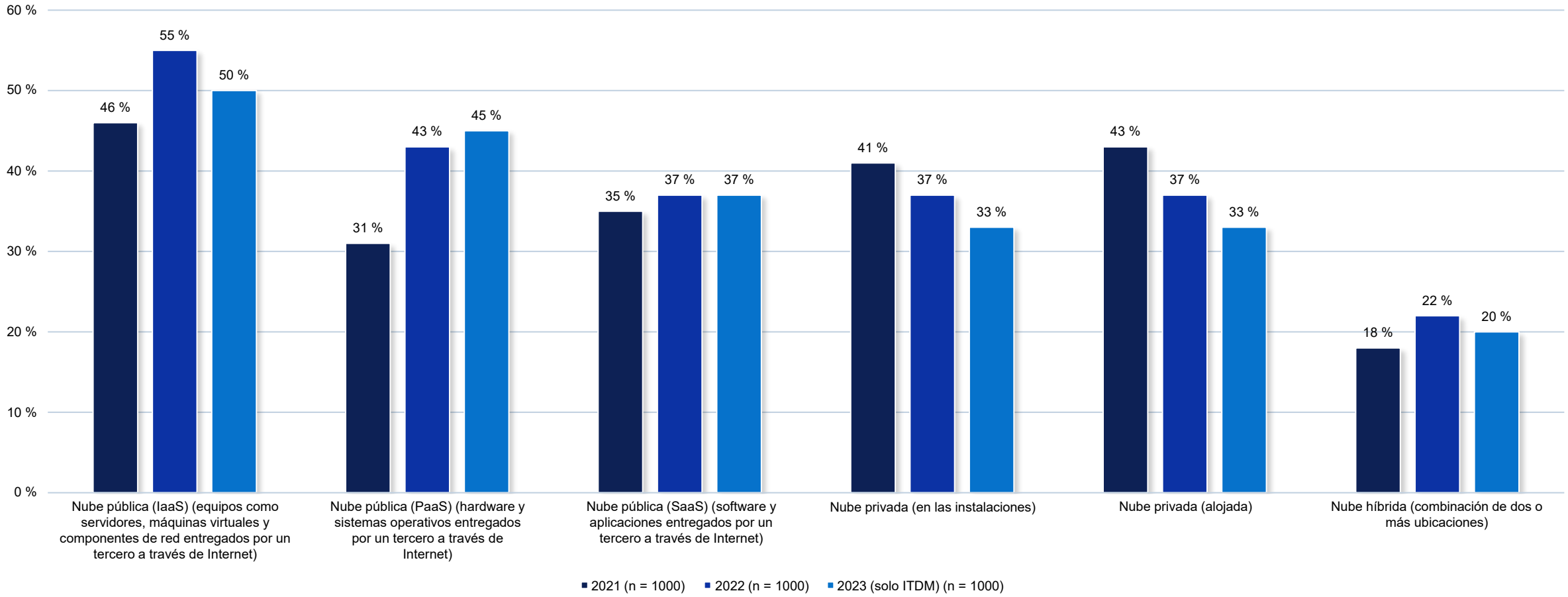
Un 85 %

afirma que si los conjuntos de datos utilizados para la IA generativa están **dañados**, afectarán **los resultados de la IA generativa**

3. El uso de las múltiples nubes

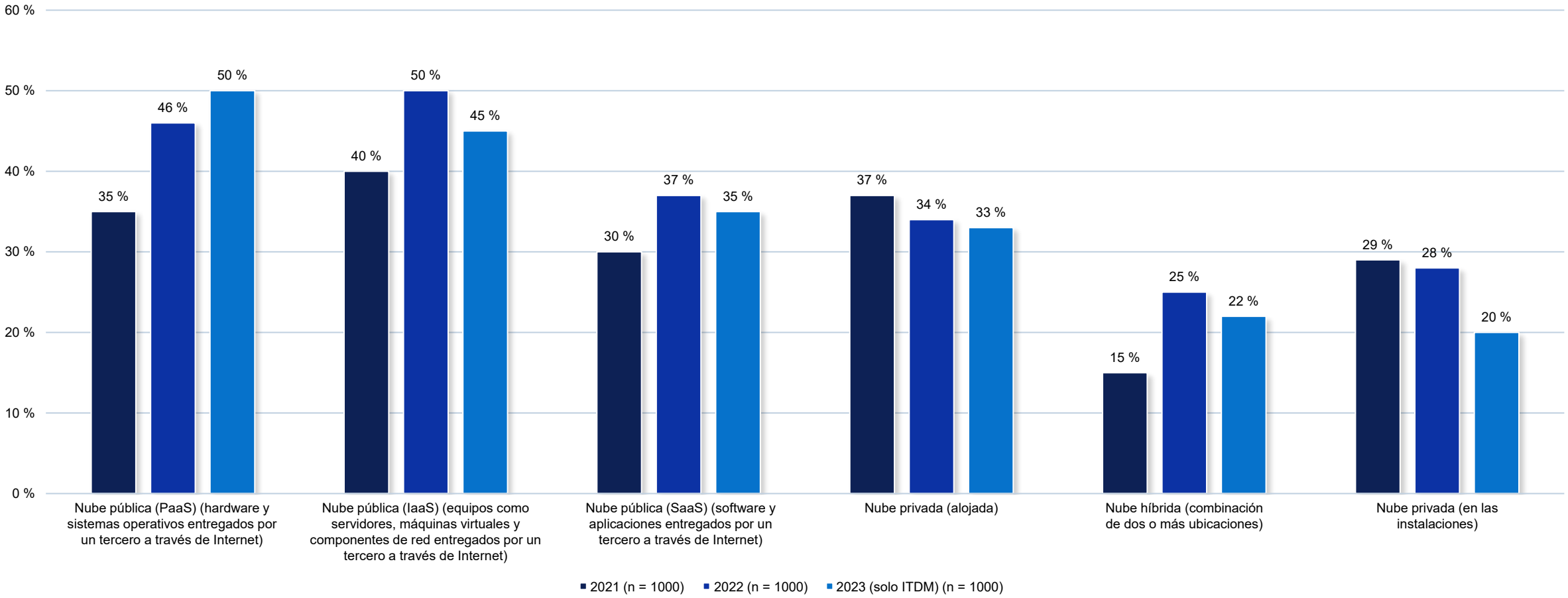
La nube pública sigue siendo una opción popular cuando se actualizan las aplicaciones existentes, mientras que la preferencia por la nube privada está disminuyendo

Medidas que se toman cuando se actualizan las aplicaciones existentes, divididas por año



La nube pública también sigue siendo una opción popular para implementar nuevas aplicaciones, pero el soporte puede estar en declive

Medidas que se toman cuando se implementan nuevas aplicaciones, divididas por año



A pesar de la popularidad de la nube pública, muchas organizaciones enfrentan desafíos para mantener sus datos

Filtro: división de datos: región = total

Debido a las preocupaciones de seguridad, muchas organizaciones están moviendo, o están considerando mover, una parte de sus cargas de trabajo a las instalaciones desde las nubes públicas

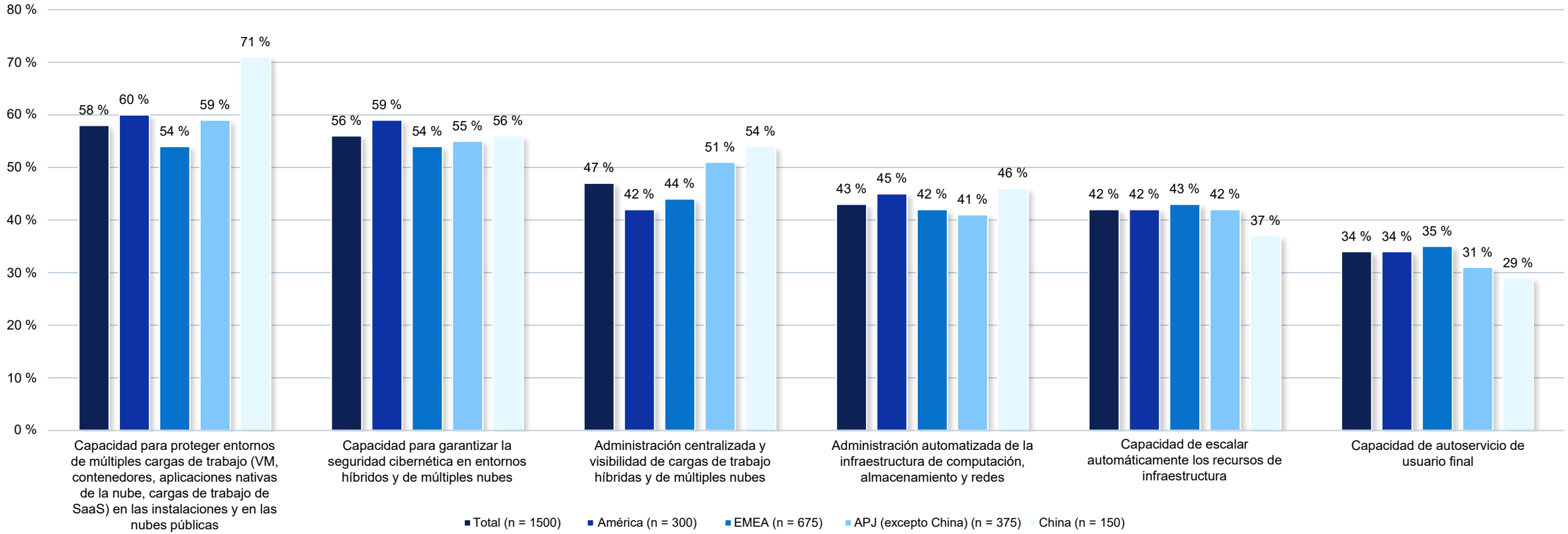
Filtro: división de datos: región = total

Un 79 %

no está muy seguro de que su organización pueda **proteger todos sus datos** en entornos de nube pública

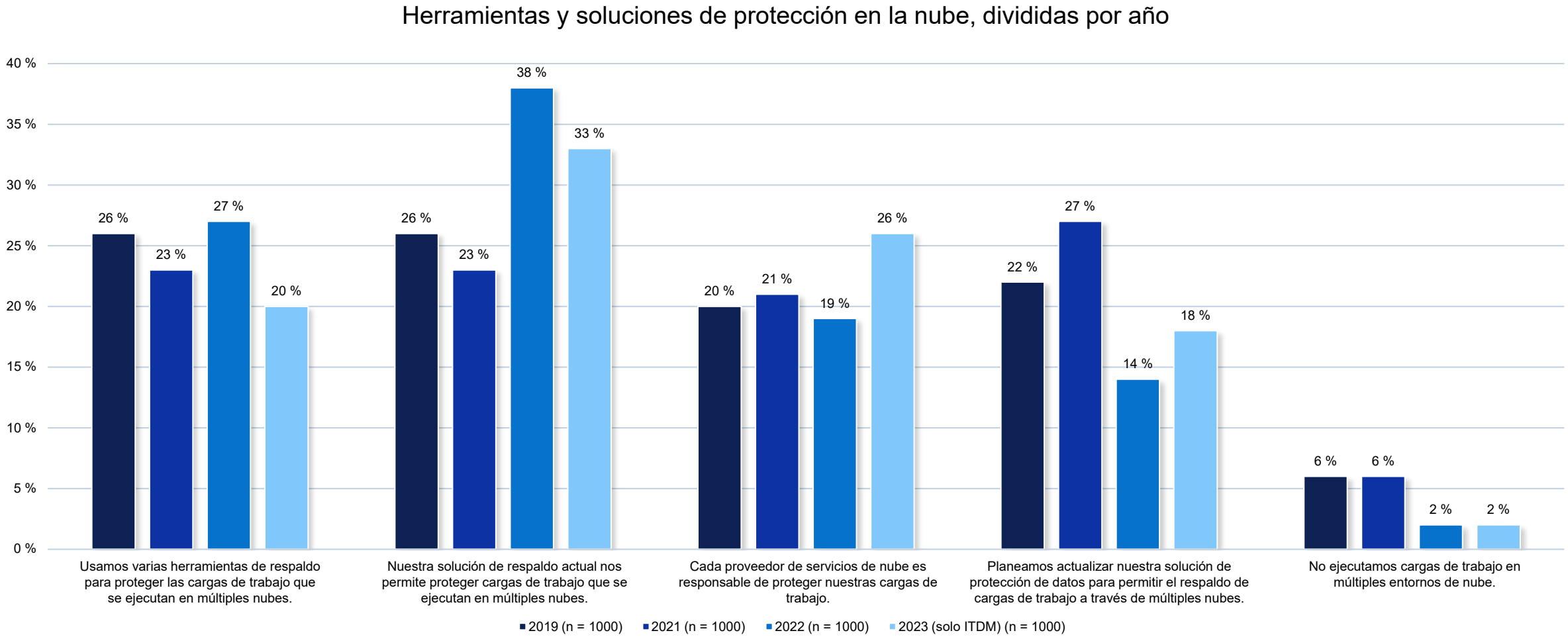
Con el aumento de los incidentes relacionados con la ciberseguridad y la escasa confianza en las estrategias de protección de datos, muchos consideran que la seguridad es la capacidad más importante a la hora de habilitar operaciones híbridas de múltiples nubes

Las capacidades más importantes a la hora de habilitar operaciones híbridas y de múltiples nubes, divididas por región



4. Protección de un entorno de nube

Actualmente, las organizaciones utilizan diversas herramientas y soluciones de respaldo para proteger sus cargas de trabajo, pero se observa la necesidad de actualizaciones



Las organizaciones dependen cada vez más de los proveedores de servicios de nube para proteger sus cargas de trabajo en todos los entornos de nube

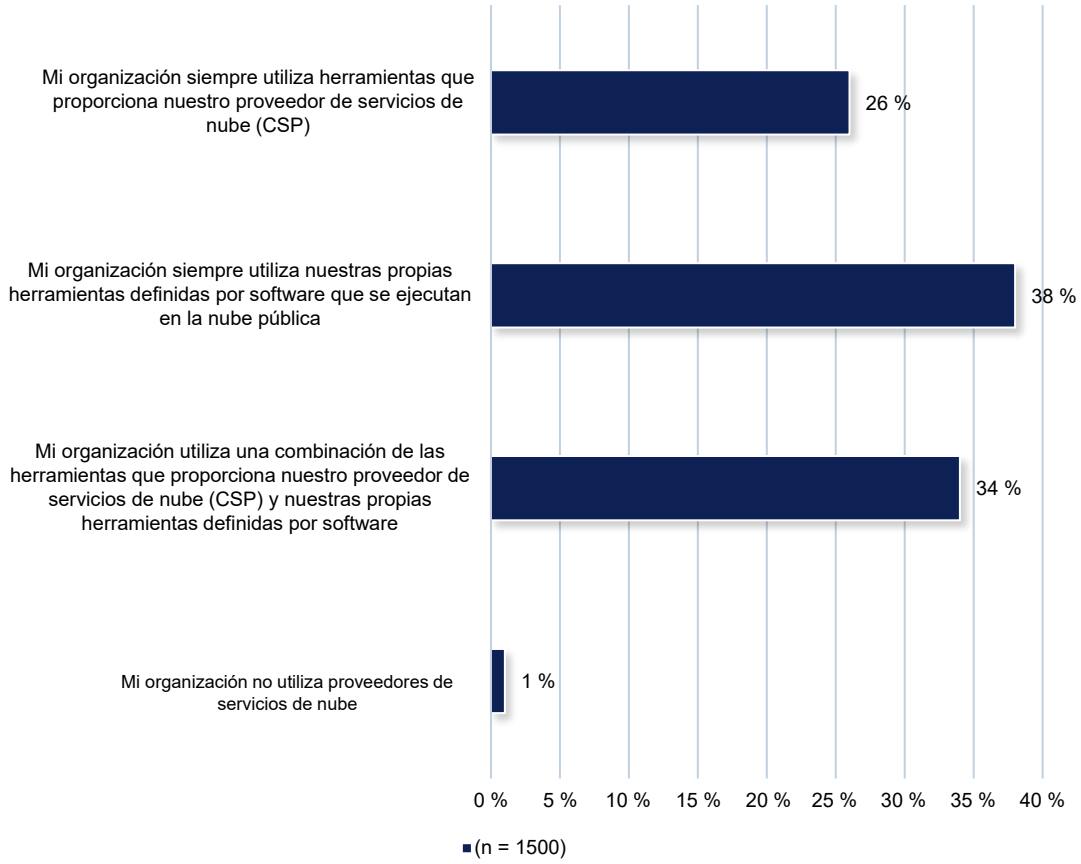
Contrato por separado con CSP para la protección de cargas de trabajo de aplicaciones

95 %

de las organizaciones **tiene un contrato por separado** con sus proveedores de servicios de nube para la **protección de las cargas de trabajo de las aplicaciones**

Filtro: división de datos: región = total

Herramientas de respaldo y recuperación proporcionadas por el proveedor de servicios de nube



Filtro: división de datos: región = total

Conclusiones clave: resumen

El panorama de riesgos de la protección de datos

- La preocupación por las medidas de protección de datos es generalizada y, ante la falta de confianza, las organizaciones se encuentran en una posición vulnerable
- Casi todas las organizaciones enfrentan desafíos relacionados con la protección de datos y muchas también sufrieron interrupciones significativas en los últimos 12 meses debido a la pérdida de datos o el tiempo de inactividad no planificado del sistema
- Las amenazas de seguridad externa fueron las causas más comunes de pérdida de datos o tiempo de inactividad no planificado de los sistemas en los últimos 12 meses
- A pesar de los desafíos y las preocupaciones por la protección de datos, pocos implementaron por completo la seguridad de confianza cero

La creciente amenaza de ataques cibernéticos

- Aumentó el número de organizaciones que sufrieron un ataque cibernético o un incidente en los últimos 12 meses, con un costo promedio para las empresas de $1,92 millones
- Muchas organizaciones están preocupadas porque los datos de respaldo de datos también podrían estar infectadas o resultar dañadas debido a ataques de ransomware.
- Además del riesgo, hay un exceso de confianza erróneo en torno a las consecuencias de un ataque de ransomware
- A pesar de que las pólizas de seguros de ransomware son comunes, se encuentran muy condicionadas, lo que deja a las organizaciones vulnerables desde el punto de vista financiero

El uso de las múltiples nubes

- La nube pública sigue siendo una opción popular cuando se actualizan las aplicaciones existentes y se implementan nuevas, pero hay preocupaciones por la seguridad de los datos
- Debido a las preocupaciones de seguridad, muchas organizaciones están moviendo, o están considerando mover, una parte de sus cargas de trabajo a las instalaciones desde las nubes públicas
- Con el aumento de los incidentes relacionados con la ciberseguridad y la escasa confianza en las estrategias de protección de datos, muchos consideran que la seguridad es la capacidad más importante a la hora de habilitar operaciones híbridas de múltiples nubes

Protección del entorno de nube

- Actualmente, las organizaciones utilizan diversas herramientas y soluciones de respaldo para proteger sus cargas de trabajo, pero reconocen que se necesitan actualizaciones
- Las organizaciones dependen cada vez más de los proveedores de servicios de nube para proteger sus cargas de trabajo en todos los entornos de nube