Índice de protección de datos global del 2021

Conclusiones clave: julio del 2021

VansonBourne

DELL Technologies

Enfoque de las conclusiones clave

1

El panorama de riesgos de la protección de datos

2

La amenaza que representan los ataques cibernéticos

3

Seguir el ritmo de las tecnologías nuevas y emergentes

4

Vulnerabilidades de la protección de datos en entornos de nube

5

El crecimiento de los modelos “como servicio”

6

Simplificar la protección de datos

Cinco puntos clave

La adopción generalizada del trabajo remoto ha **aumentado los riesgos cibernéticos y de protección de datos**

Muchos no confían en la capacidad de protección de datos de su organización para defenderse y recuperarse de las amenazas cibernéticas

Las inversiones continuas en tecnologías emergentes y la nube **pueden contribuir a los desafíos de la protección de datos**

Muchos **están interesados en aprovechar el modelo "como servicio"** para aumentar la simplicidad y flexibilidad de la protección de datos

Existe evidencia de que trabajar con **menos proveedores de protección de datos** se correlaciona con **mejores resultados de protección de datos**

¿A quiénes entrevistamos?

1000 tomadores de decisiones de TI fueron entrevistados en febrero, marzo y abril de 2021

Organizaciones de una amplia variedad de industrias del sector público y privado

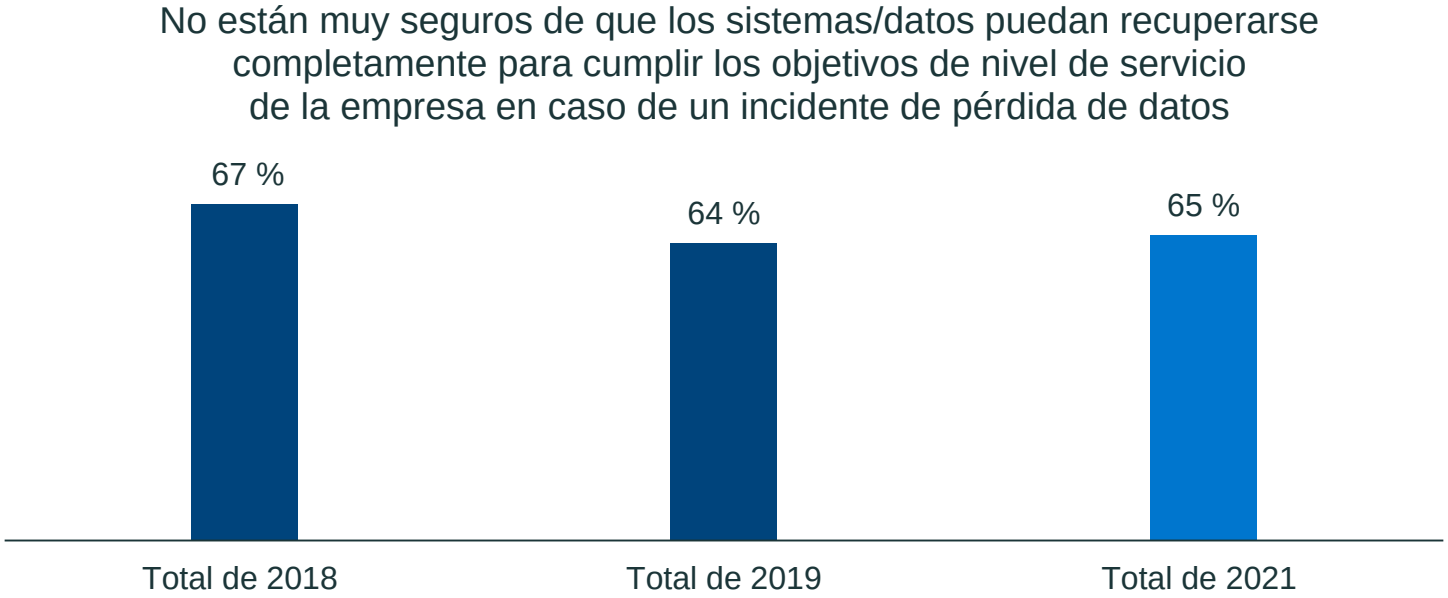
Organizaciones que tienen más de 250 empleados

4 regiones:

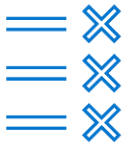
América (200)
EMEA (450)
APJ (250)
China (100)

1. El panorama de riesgos de la protección de datos

Los tomadores de decisiones de TI no confían en la capacidad de su organización para cumplir los SLO de recuperación



Además, la confianza en que las capacidades de protección de datos están a la altura de las normas internas y externas es baja, lo que resulta más preocupante por el hecho de que dos tercios creen que experimentarán un evento disruptivo el próximo año.



58 %

no están muy seguros de que su organización esté **cumpliendo con los objetivos de nivel de servicio de respaldo y recuperación**

63 %

no están muy seguros de que la infraestructura y los procesos actuales de protección de datos de su organización **cumplan con las regulaciones regionales de gestión de datos**

64 %

están **preocupados por la posibilidad de sufrir un evento disruptivo** en los próximos doce meses

A este motivo de preocupación se suma que los problemas de pérdida de datos y tiempo de inactividad de los sistemas continúan teniendo un impacto financiero significativo en las organizaciones

US$ 959 493

Costo promedio de la pérdida de datos en los últimos 12 meses (en USD)

US$ 513 067

Costo promedio del tiempo de inactividad no planificado de los sistemas en los últimos 12 meses (en USD)

2. La amenaza que representan los ataques cibernéticos

Las organizaciones no confían en que sus medidas de protección de datos puedan mitigar los efectos de los ataques cibernéticos. Además, la mayoría cree que la exposición es mayor debido a los empleados que trabajan desde casa

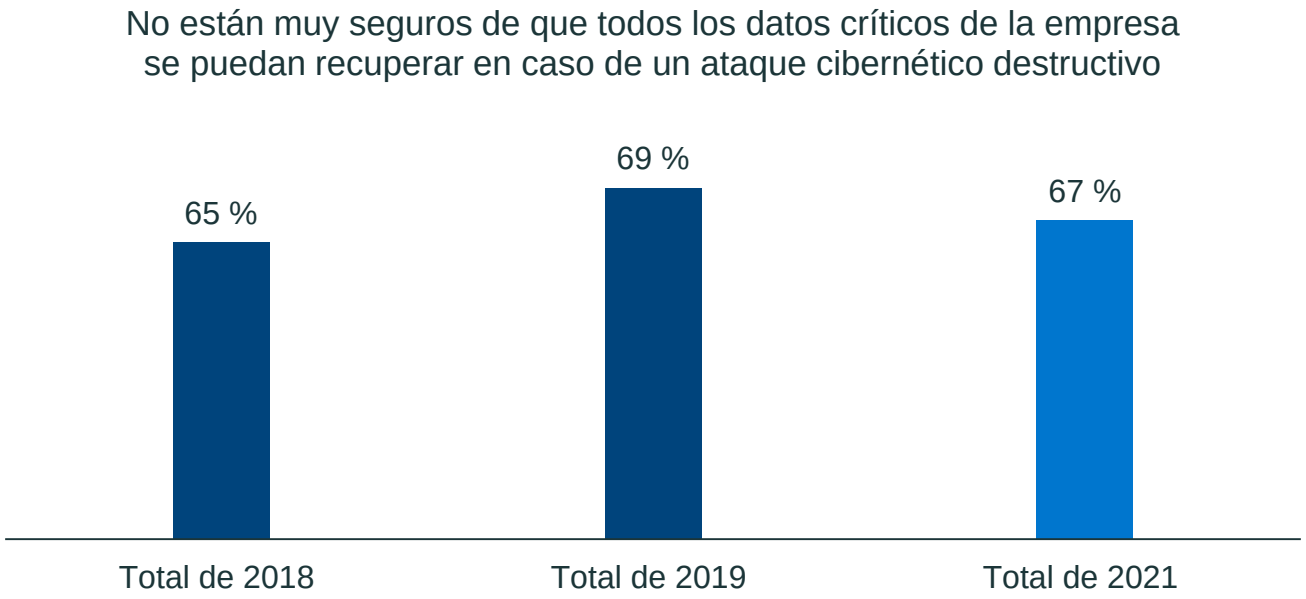
62 %

les preocupa que las medidas de protección de datos existentes de su organización **no sean suficientes para enfrentar las amenazas de malware y ransomware**

74 %

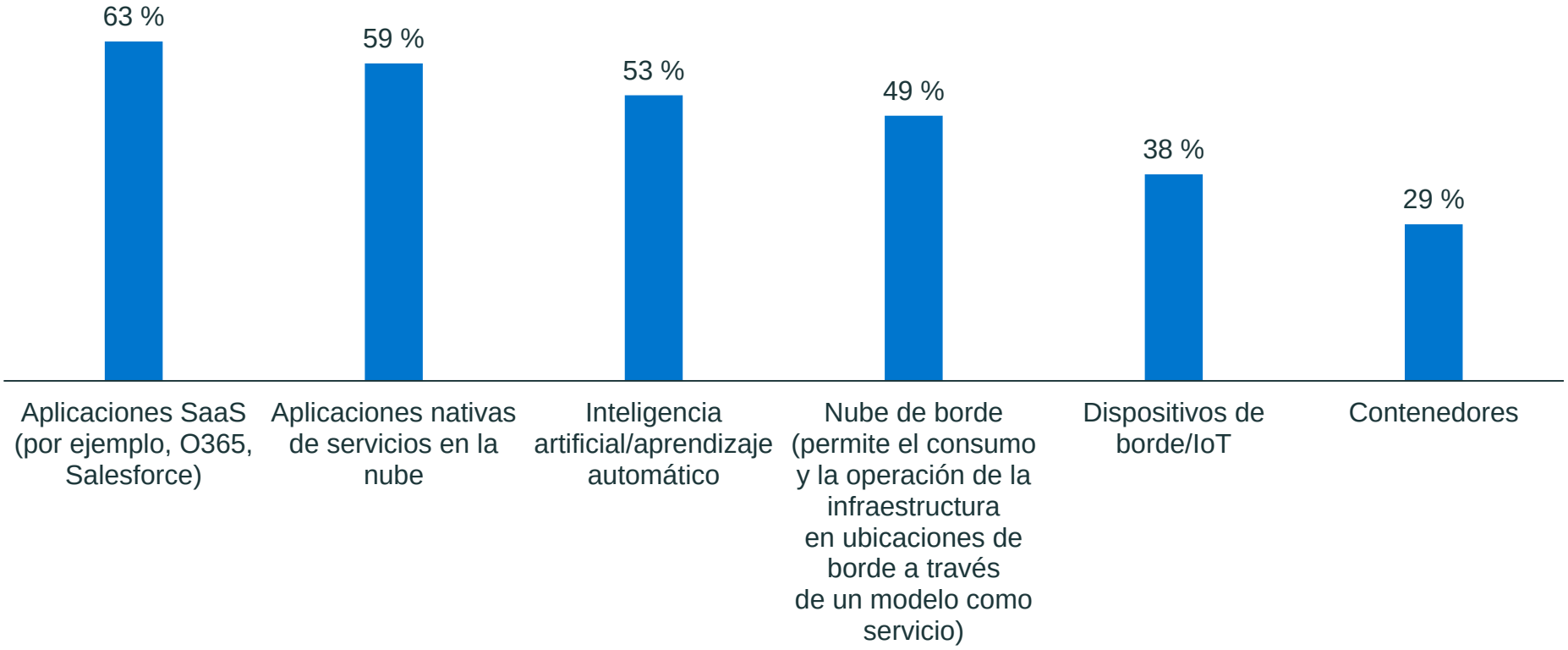
están de acuerdo en que su organización **está más expuesta a la pérdida de datos** a causa de las amenazas cibernéticas con el aumento de **empleados que trabajan desde casa**

Además de la preocupación por la capacidad de las organizaciones para enfrentar las amenazas de malware y ransomware, muchas no creen que sea posible recuperar todos los datos críticos de la empresa en caso de un ataque cibernético destructivo

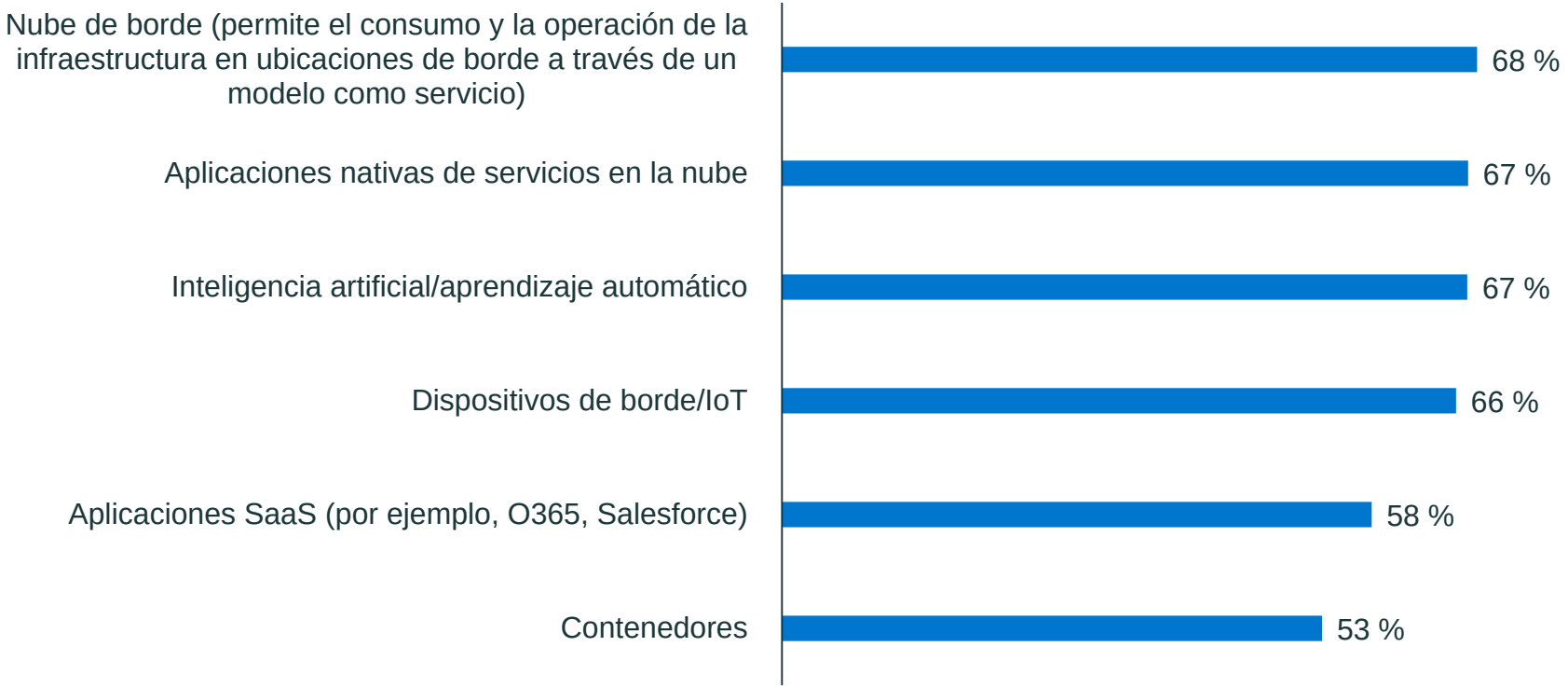


3. Seguir el ritmo de las tecnologías nuevas y emergentes

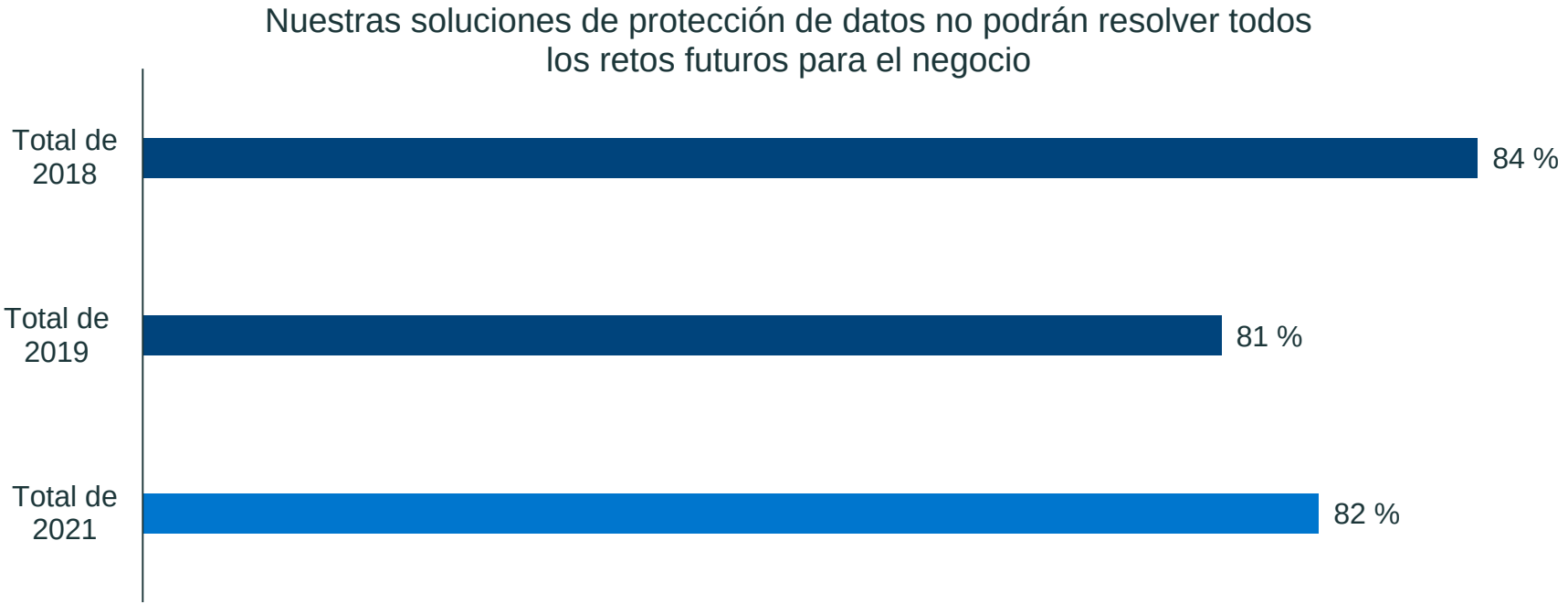
Las organizaciones están invirtiendo en muchas tecnologías nuevas, lo que podría complicar sus desafíos de protección de datos



Muchas organizaciones tienen problemas para proteger estas tecnologías



Es probable que la dificultad para proteger tecnologías nuevas y emergentes contribuya a la poca confianza en que las soluciones de protección de datos están preparadas para el futuro



Muchos ven las tecnologías emergentes como un riesgo para la protección de datos y la preocupación por futuros eventos disruptivos es alta, especialmente en aquellos que utilizan varios proveedores de protección de datos.

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

Usan un único proveedor de protección de datos

57 %

Usan varios proveedores de protección de datos

64 %

Me preocupa que experimentemos un evento disruptivo (por ejemplo, pérdida de datos, tiempo de inactividad en los sistemas, etc.) en los próximos 12 meses

Usan un único proveedor de protección de datos

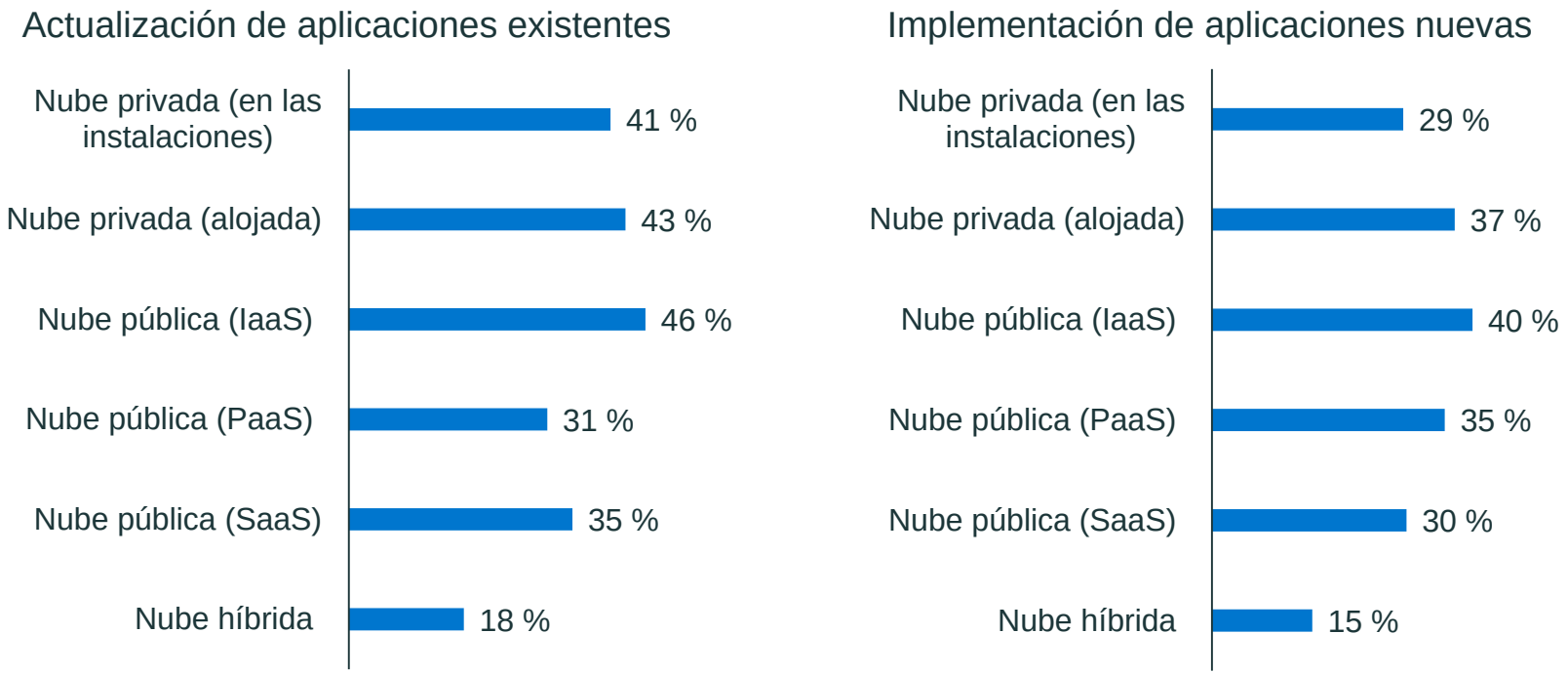
54 %

Usan varios proveedores de protección de datos

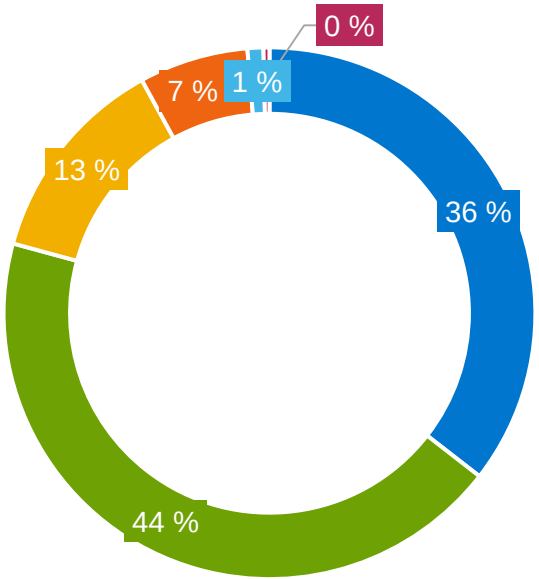
68 %

4. Vulnerabilidades de la protección de datos en entornos de nube

Las aplicaciones se actualizan e implementan en una variedad de entornos en las infraestructuras de TI de las organizaciones



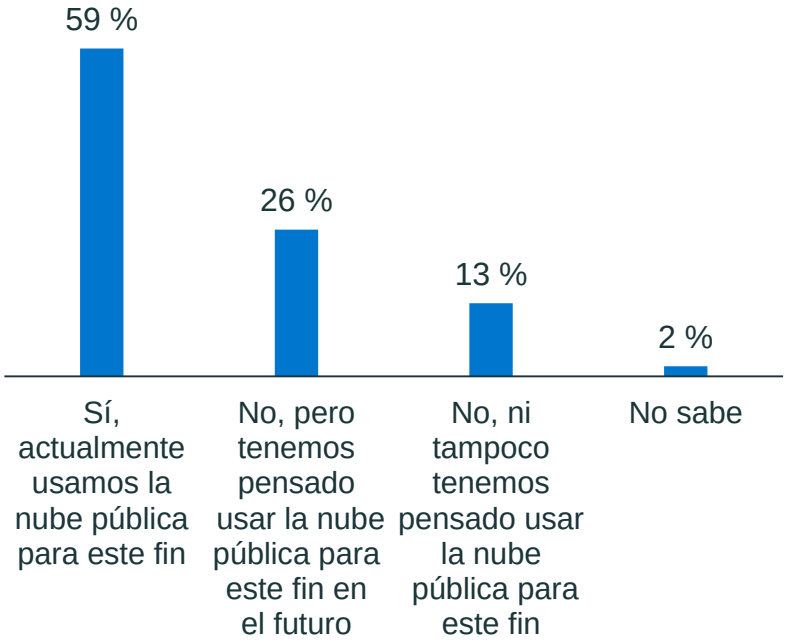
Sin embargo, muchos no están seguros de su capacidad de protección de datos en entornos de nube pública



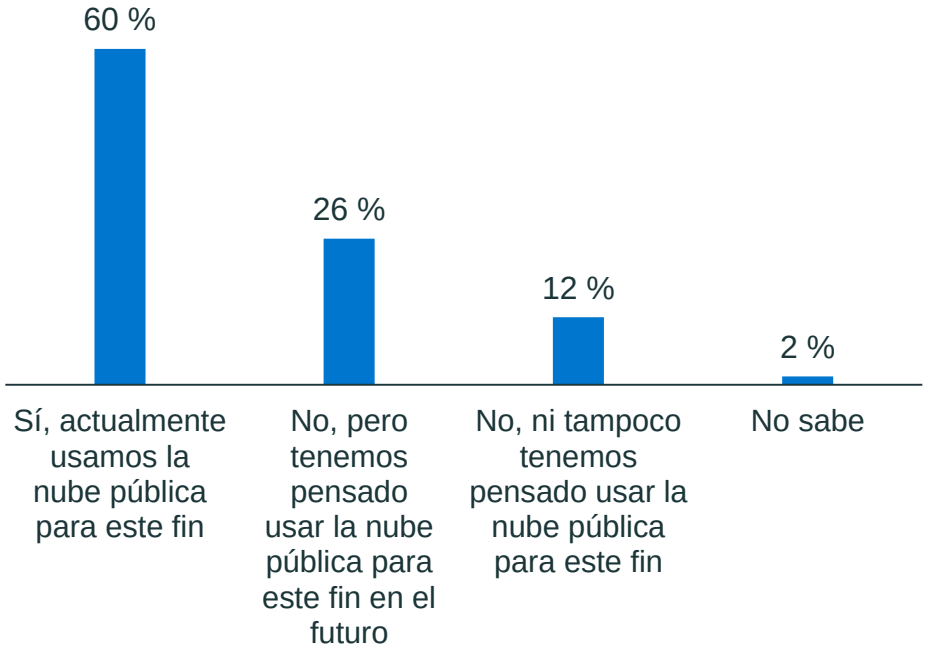
- Muy seguro: todos los datos están protegidos en la nube pública
- Moderadamente seguro: los datos cruciales están protegidos en la nube pública, pero no la totalidad de los datos
- Tengo algunas dudas: la mayoría de los datos están protegidos en la nube pública
- No muy seguro: algunos datos cruciales están protegidos en la nube pública
- Para nada seguro: los datos no están protegidos en la nube pública
- No sé

La nube pública tiene un papel cada vez más importante en las estrategias de recuperación ante desastres y retención a largo plazo de las organizaciones

Recuperación ante desastres



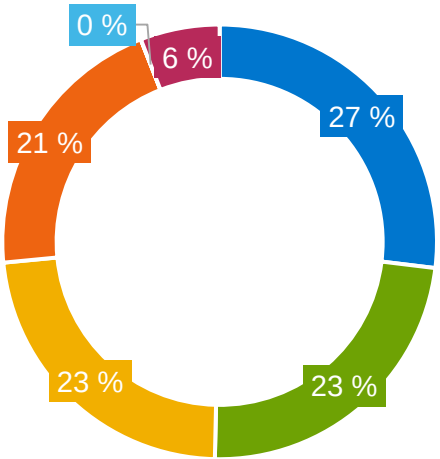
Retención a largo plazo



Varias organizaciones que utilizan múltiples entornos de nube no utilizan soluciones específicas para protegerlos

21 %

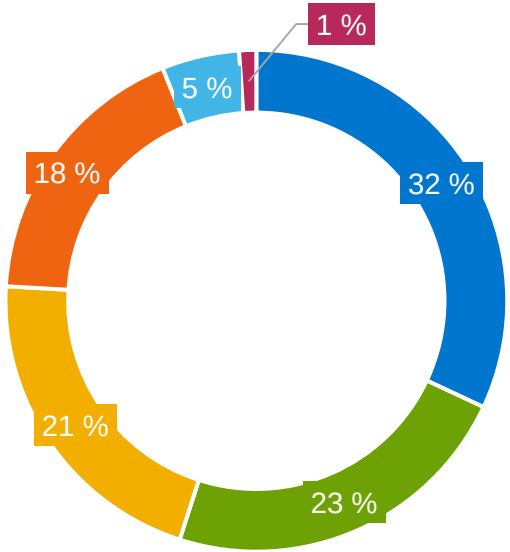
creen que, cuando se utilizan varios entornos de nube, **cada proveedor de servicios de nube** es responsable de **proteger sus cargas de trabajo**



- Planeamos actualizar nuestra solución de protección de datos para permitir el respaldo de cargas de trabajo a través de múltiples nubes.
- Nuestra solución de respaldo actual nos permite proteger cargas de trabajo que se ejecutan en múltiples nubes.
- Usamos varias herramientas de respaldo para proteger las cargas de trabajo que se ejecutan en múltiples nubes.
- Cada proveedor de servicios de nube es responsable de proteger nuestras cargas de trabajo.
- Otros
- No ejecutamos cargas de trabajo en múltiples entornos de nube.

Lo mismo ocurre cuando se considera proteger las cargas de trabajo virtualizadas con VMware en la nube

- Planeamos actualizar nuestra solución de protección de datos para permitir tener un respaldo de las cargas de trabajo de VMware en la nube híbrida.
- Nuestro proveedor de servicios de nube es responsable de proteger nuestras cargas de trabajo.
- Con las herramientas de respaldo que usamos y operamos actualmente en las instalaciones
- Con herramientas de respaldo disponibles en el mercado de proveedores de servicio de nube
- No ejecutamos cargas de trabajo virtualizadas con VMware en la nube ni pensamos hacerlo
- No sabe

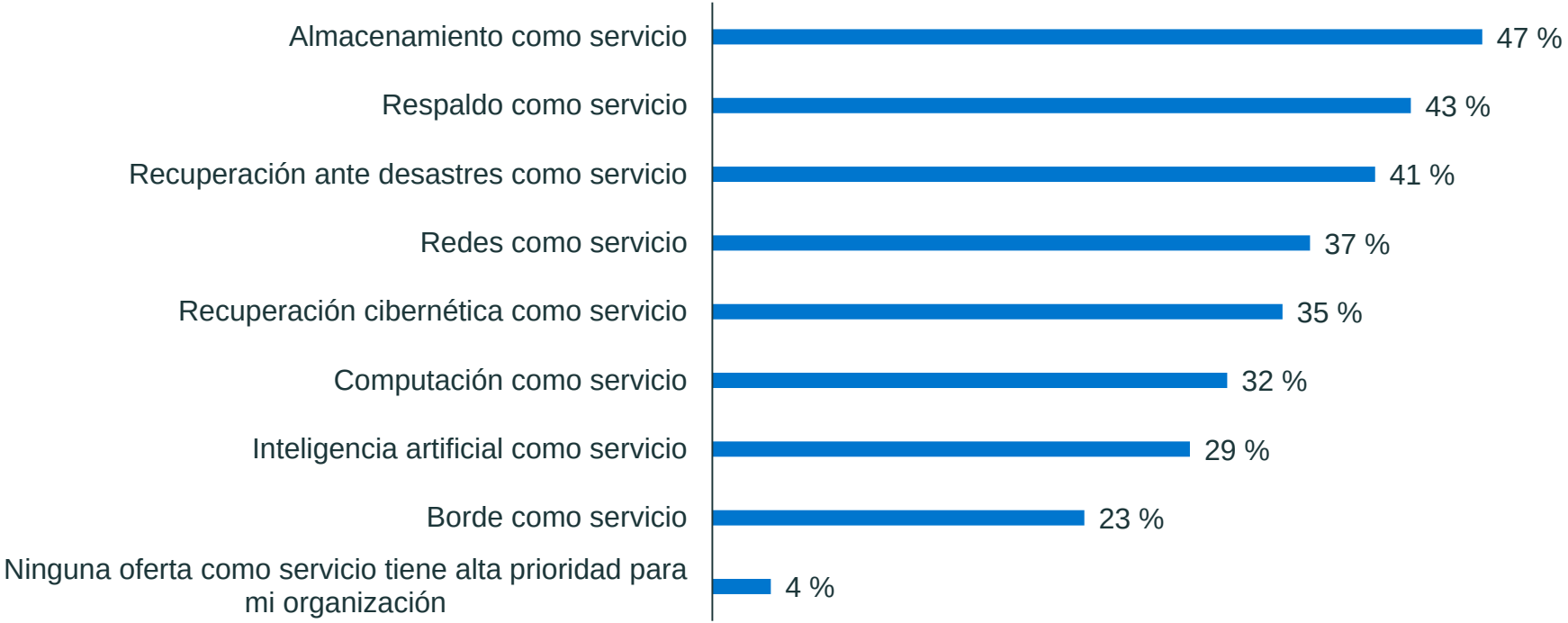


23 %

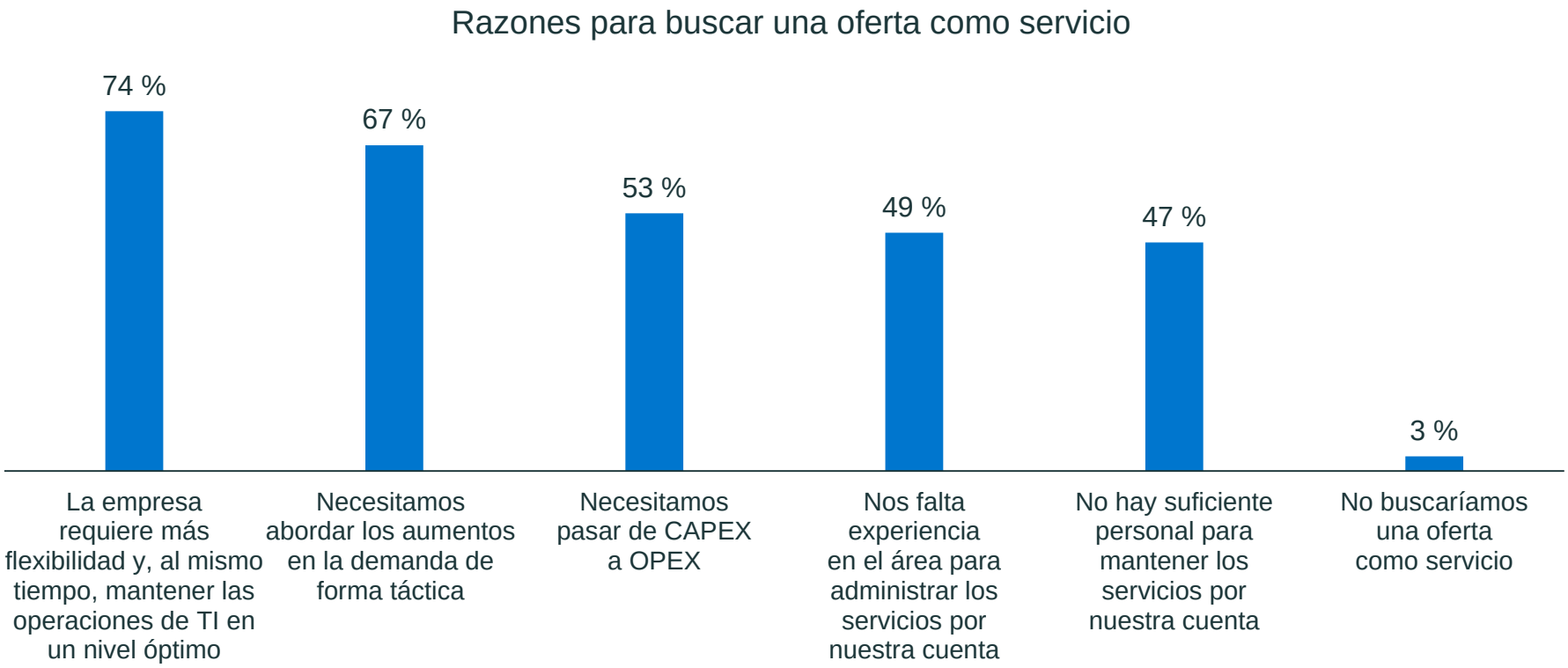
creen que el **proveedor de servicios de nube** es responsable de **proteger sus cargas de trabajo virtualizadas**

5.El crecimiento de los modelos “como servicio”

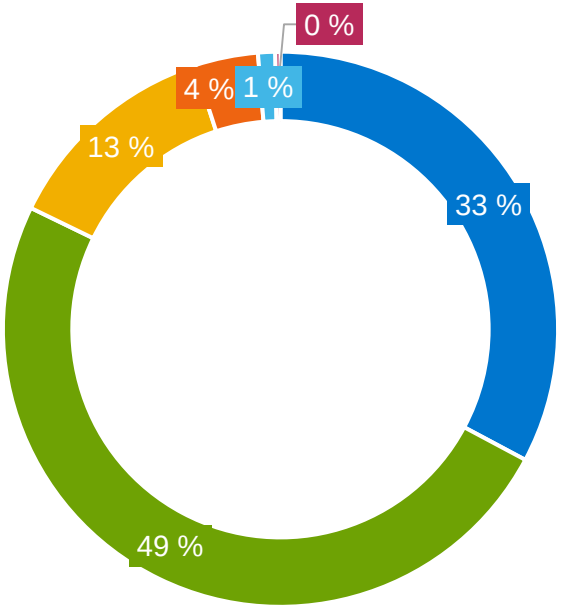
La mayoría de las organizaciones priorizan las ofertas como servicio: el respaldo como servicio y la recuperación ante desastres como servicio se encuentran entre las que tienen mayor prioridad



La popularidad de las ofertas como servicio suele deberse a su flexibilidad



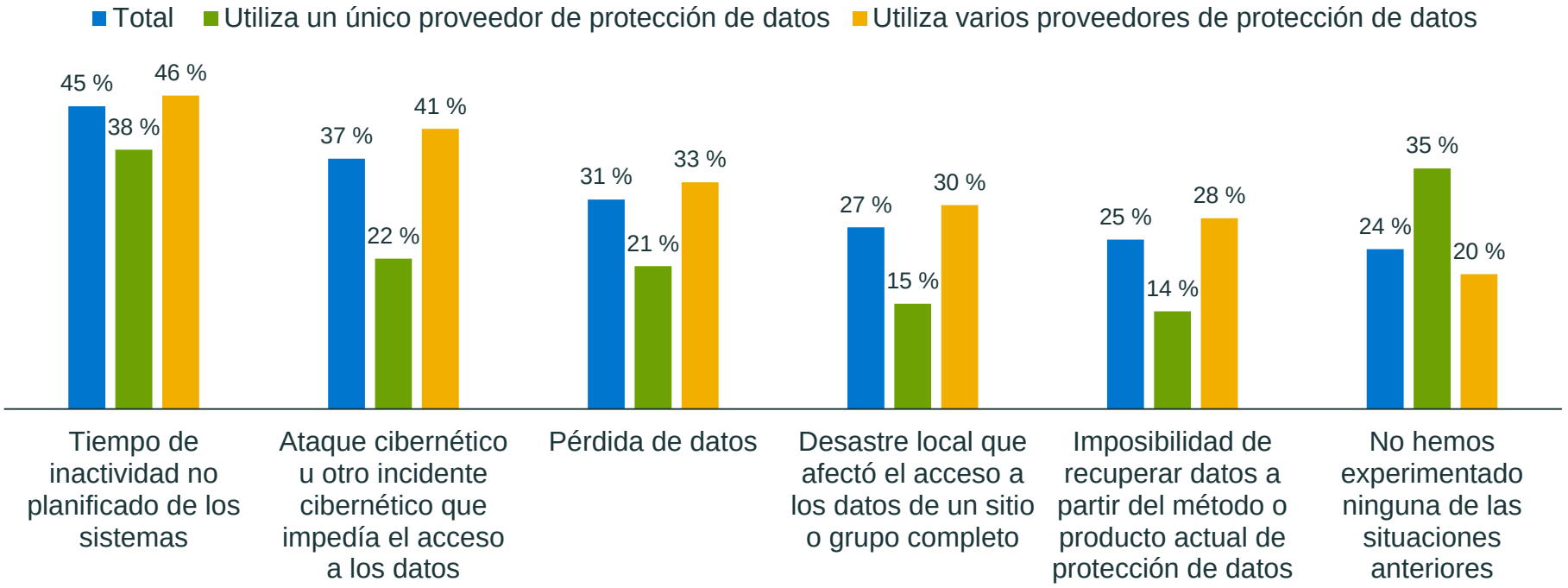
La gran mayoría preferiría trabajar con un proveedor que tenga varias ofertas como servicio, lo que sugiere que existe un deseo de consolidar las cargas de trabajo con menos proveedores



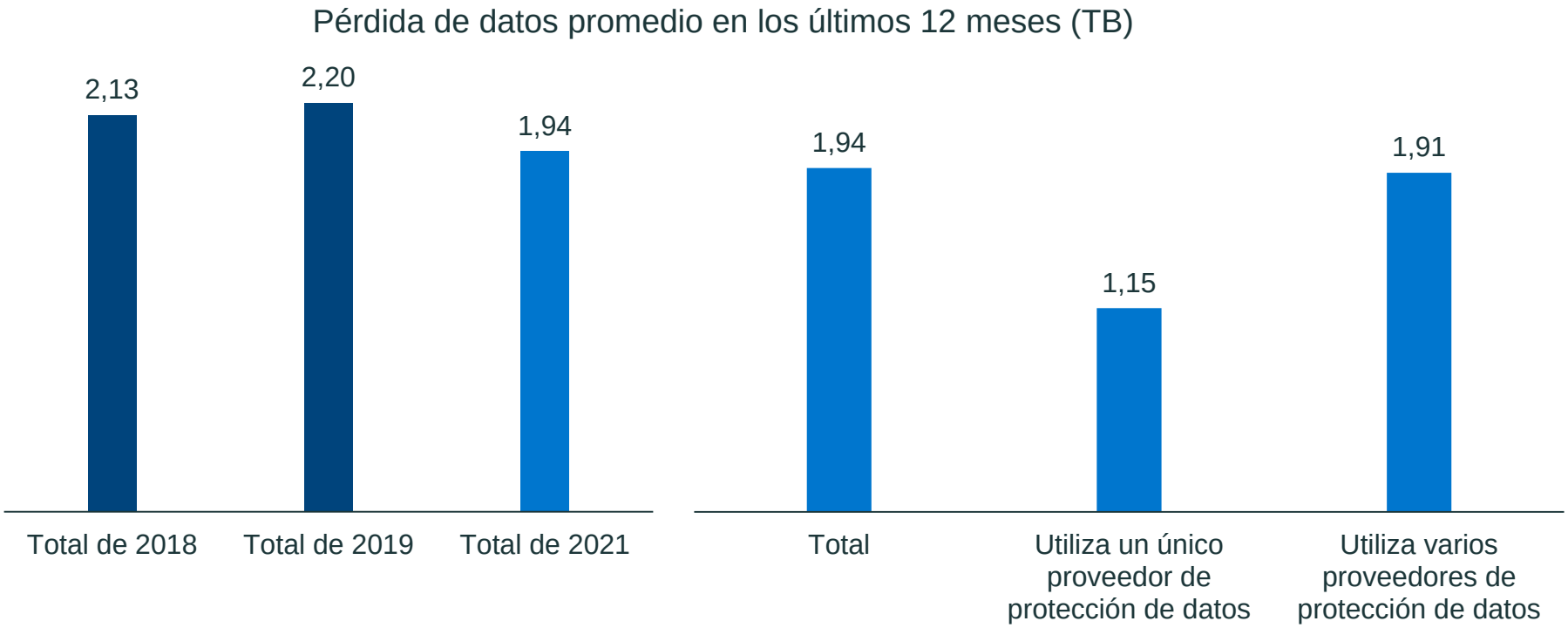
- Es bastante probable que busquemos un proveedor que tenga varias ofertas como servicio
- Es probable que busquemos un proveedor que tenga varias ofertas como servicio
- Me es indiferente si un proveedor tiene varias ofertas como servicio
- Es poco probable que busquemos un proveedor que tenga varias ofertas como servicio
- Es muy poco probable que busquemos un proveedor que tenga varias ofertas como servicio
- No sé

6. Simplificar la protección de datos

Es más probable que las organizaciones que utilizan varios proveedores de protección de datos hayan sufrido problemas relacionados con la pérdida de datos, el acceso a los datos o el tiempo de inactividad de los sistemas en el último año en comparación con aquellas que utilizan un único proveedor



En promedio, las organizaciones que utilizan varios proveedores de protección de datos pierden más datos que las que utilizan un único proveedor



Conclusiones clave: resumen (1/2)

El panorama de riesgos de la protección de datos

- A muchos les preocupa no poder recuperar todos los sistemas/datos para cumplir con los SLO en caso de un incidente de pérdida de datos
- El temor de las organizaciones de experimentar un evento disruptivo en los próximos doce meses es generalizado y las consecuencias de estos eventos disruptivos podrían ser devastadoras desde el punto de vista financiero
- Las organizaciones deben tomar medidas a fin de asegurarse de estar preparadas para reaccionar ante estos eventos si ocurren

La amenaza que representan los ataques cibernéticos

- Existe una gran preocupación por el hecho de que las organizaciones no puedan protegerse contra las amenazas de malware y ransomware, y la mayoría coinciden en que el riesgo de ataques cibernéticos ha aumentado con el incremento del trabajo remoto
- Si las organizaciones sufren ataques, pocos confían en que su organización pueda recuperar todos los datos cruciales de la empresa

Seguir el ritmo de las tecnologías nuevas y emergentes

- Las organizaciones están invirtiendo en una variedad de tecnologías nuevas y emergentes, entre las que se incluyen aplicaciones SaaS, IA/ML y dispositivos de borde/IoT, pero suelen tener problemas para garantizar que la protección de datos se mantenga actualizada
- Muchos creen que estas tecnologías suponen un riesgo para la protección de datos, y es probable que estos riesgos contribuyan al temor de que las organizaciones no estén preparadas para el futuro y corran el riesgo de sufrir interrupciones en los próximos doce meses
- Las inversiones en tecnologías emergentes son algo positivo y deben fomentarse, pero las organizaciones deben asegurarse de que su infraestructura de protección de datos sea compatible con estas tecnologías

Conclusiones clave: resumen (2/2)

Vulnerabilidades de la protección de datos en entornos de nube

- Las aplicaciones se actualizan e implementan en una variedad de entornos de nube, pero suele faltar confianza en lo que respecta a la capacidad de proteger los datos
- La nube desempeña un papel importante en las estrategias de recuperación ante desastres y retención a largo plazo
- Las organizaciones deben asegurarse de tener soluciones específicas para proteger los datos en cargas de trabajo virtualizadas y de múltiples nubes, ya que algunas empresas todavía creen que los proveedores de servicio en la nube son responsables de esto

El crecimiento de los modelos “como servicio”

- Las soluciones como servicio son de interés para la mayoría de las organizaciones y, probablemente, formen parte de las soluciones de protección de datos de muchas empresas en el futuro. Por lo general, la flexibilidad es una de las razones clave de este interés
- La preferencia de la mayoría es utilizar soluciones como servicio de proveedores con varias ofertas, una opción que podría ayudar a simplificar la protección de datos para estas organizaciones

Simplificar la protección de datos

- Es más probable que las organizaciones que utilizan un único proveedor de protección de datos hayan experimentado pérdidas de datos, problemas de acceso a los datos e incidentes de tiempo de inactividad no planificados en los sistemas en el último año en comparación con aquellas que utilizan varios proveedores
- En promedio, aquellas que utilizan un solo proveedor han perdido menos datos que las que utilizan varias soluciones
- Si bien las organizaciones pueden verse tentadas a ampliar sus capacidades de protección de datos invirtiendo en nuevas soluciones, es probable que estén mejor protegidas contra la pérdida de datos y el tiempo de inactividad si consolidan sus soluciones con un único proveedor

Mitigar el riesgo y adelantarse a los acontecimientos

Punto de vista de Dell Technologies

Realizar revisiones periódicas de la preparación de la protección de datos

Priorizar la resiliencia cibernética de manera absoluta

Consolidar las iniciativas de protección de datos con Dell

Visite DellTechnologies.com/GDPI para obtener más información


DELL Technologies