Global Data Protection Index

Cyber Resiliency Multicloud Edition

DELL Technologies

Tabla de contenidos

Introducción 3

El panorama de riesgos de la protección de datos 4

La creciente amenaza de los ataques cibernéticos 4

Costo de los ataques cibernéticos 5

Los riesgos del trabajo remoto 6

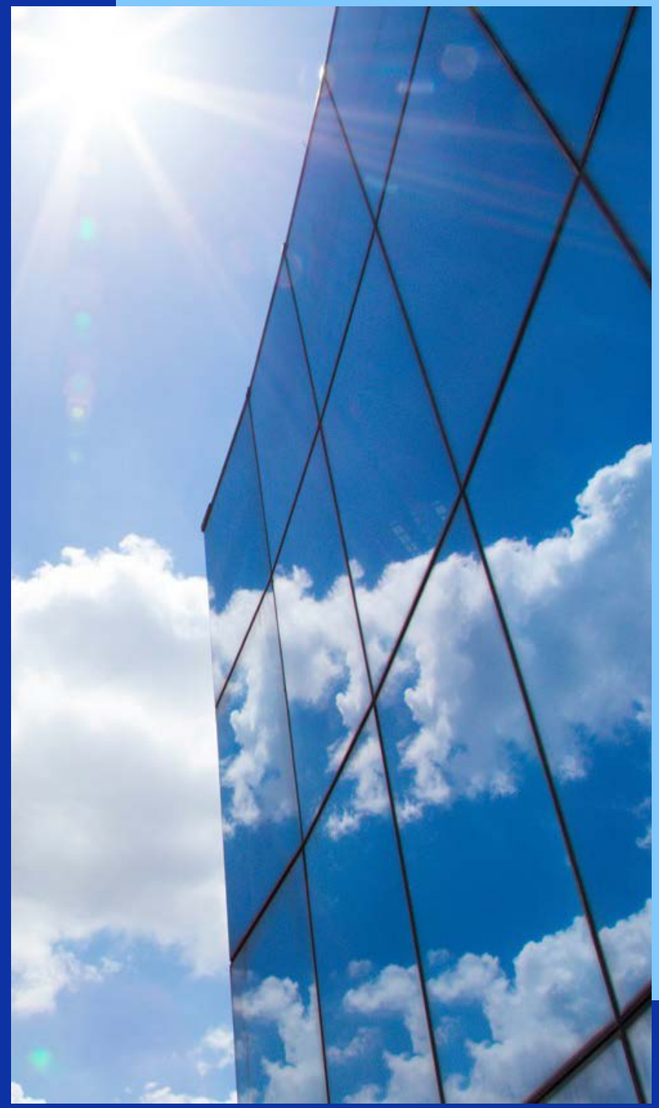
Políticas de ransomware 7

IA generativa y ciberseguridad 8

El uso de las múltiples nubes 9

Protección de un entorno de múltiples nubes 10

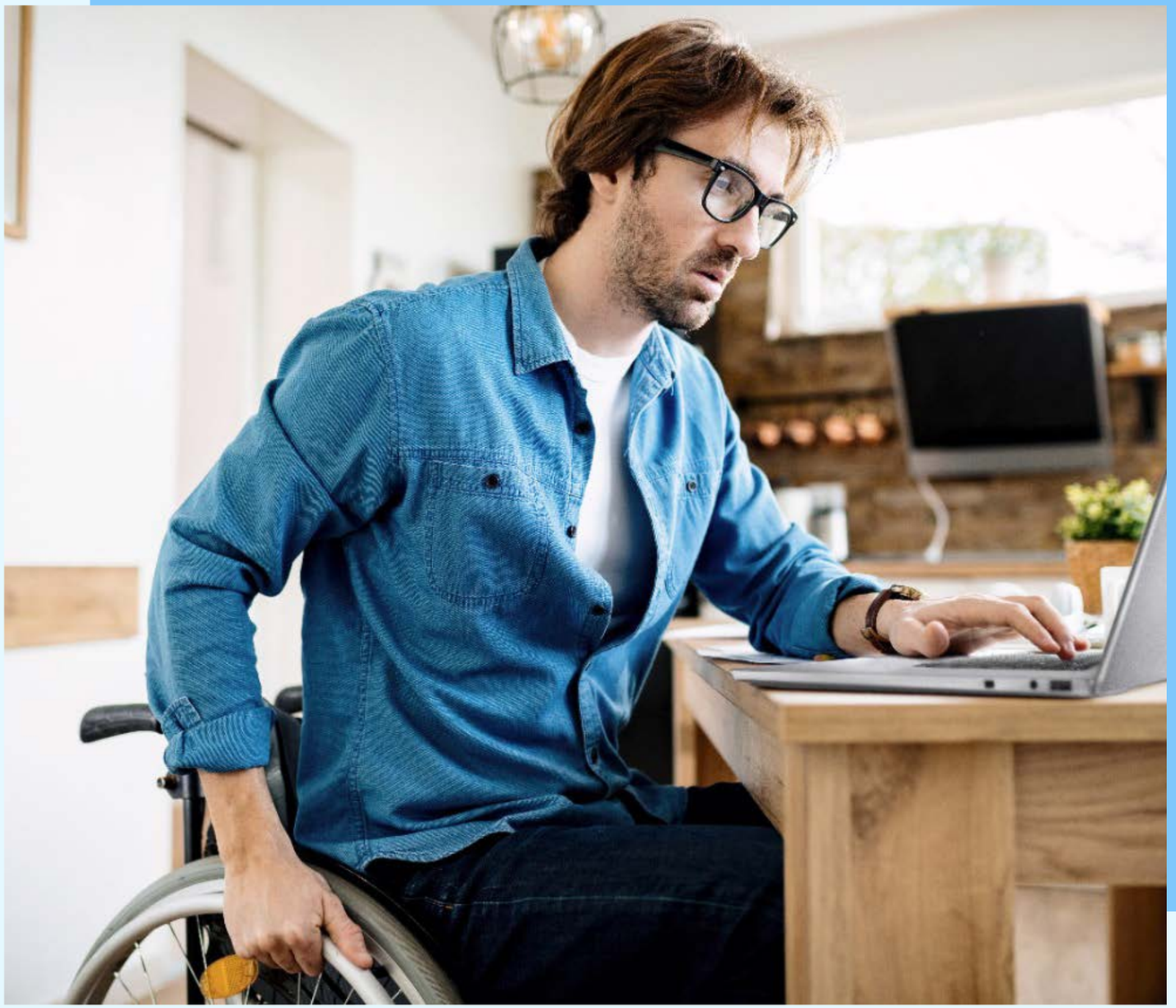
Conclusión 11



Introducción

En el mundo actual transformado digitalmente, la función crucial de los datos en la estrategia de negocios lo convierte en un objetivo principal para escalar las amenazas cibernéticas. El surgimiento de la IA generativa y la expansión hacia entornos híbridos y de múltiples nubes elevaron estos riesgos, con ataques cibernéticos que causan daños financieros significativos, que se duplican desde el año anterior a un promedio de $1,4 millones. En medio de esto, las organizaciones enfrentan los desafíos de proteger y asegurar sus recursos de nube cada vez más complejos, lo que destaca la necesidad vital de estrategias sólidas de protección de datos resistentes cibernéticos en este panorama en constante evolución.

En este e-Book, se presentan las conclusiones del Global Data Protection Index de 2024 de Dell Technologies encargado por Vanson Bourne, una encuesta realizada a 1000 tomadores de decisiones de TI y 500 tomadores de decisiones de seguridad de TI en todo el mundo. A menos que se especifique lo contrario, solo se hace referencia a los resultados de los 1000 tomadores de decisiones de TI cuando se realizan comparaciones históricas.



El panorama de riesgos de la protección de datos

Navegar por el complejo terreno de la protección de datos sigue siendo un desafío fantástico para las organizaciones, un obstáculo que impacta directamente en su viaje hacia la transformación digital. La gran mayoría (90 %) de las organizaciones han experimentado algún tipo de interrupción en los últimos 12 meses.

Esta interrupción generalizada no se pierde en los líderes de TI y seguridad de TI. El 79 % expresa su preocupación por posibles eventos disruptivos en el próximo año.

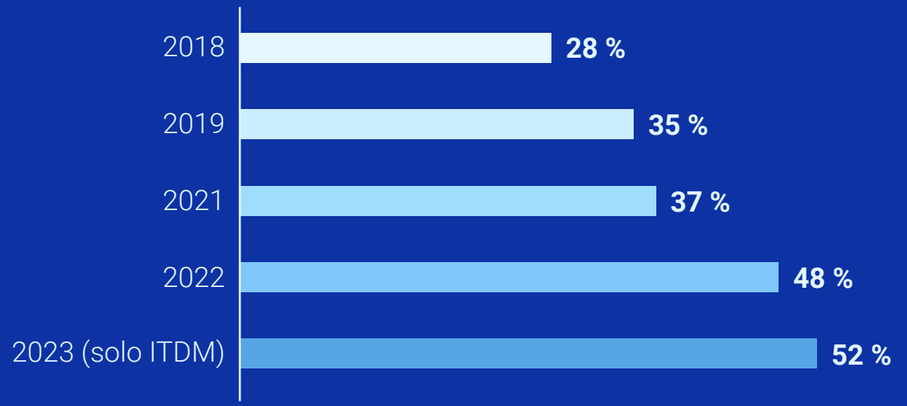
Estas inquietudes están eclipsando su confianza en el logro de los objetivos de nivel de servicio (SLO) de respaldo y recuperación y el 60 % no se siente "muy seguro" de las capacidades de su organización en esta área.

Además de estas preocupaciones, los eventos de pérdida de datos tienen un impacto financiero significativo en las organizaciones, con un costo promedio de USD $2,61 millones en los últimos 12 meses.

ITC

La amenaza de los ataques cibernéticos sigue creciendo, por lo que sigue estando primero en la lista de causas de interrupción organizacional por segundo año consecutivo. Más de la mitad (52 %) de los tomadores de decisiones de TI informan que su organización ha sufrido un ataque cibernético o un incidente que impedía el acceso a los datos en los últimos 12 meses.

Ataque cibernético u otro incidente cibernético que impedía el acceso a los datos



Los cibercriminales apuntan a una variedad de puntos de entrada, pero es más probable que los ataques provengan de fuentes externas. De hecho, el primer punto de entrada del 55 % de los atacantes fue externo: los usuarios que hacen clic en correos electrónicos de spam o phishing y enlaces maliciosos, credenciales de usuario vulneradas y dispositivos móviles hackeados.

El costo de los ataques cibernéticos

Esto tiene un impacto financiero considerable en las organizaciones, ya que los costos asociados con los ataques cibernéticos y otros incidentes relacionados con estos se duplicaron en los últimos 12 meses:

2022
US$660 000

↑

2023 (solo ITDM)
US$1 410 000

Además, las violaciones de seguridad externas son las causas más mencionadas de pérdida de datos o tiempo de inactividad de los sistemas dentro de las organizaciones

40 %

El riesgo del trabajo remoto

A pesar de la popularidad del trabajo remoto e híbrido, las organizaciones se encuentran en una posición precaria. Más de ocho de cada diez (81 %) ahora creen que tienen una mayor exposición a la pérdida de datos por amenazas cibernéticas debido al crecimiento de los empleados que trabajan desde el hogar.

Hemos aumentado la exposición a la pérdida de datos por amenazas cibernéticas con el aumento de los empleados que trabajan desde el hogar

2022 **70 %** → **2023** (solo ITDM) **81 %**

Resumen: Combinación de "Totalmente de acuerdo" y "De acuerdo"

Para agregar preocupaciones, un cantidad cada vez mayor coincide en que las medidas de protección de datos existentes en su organización pueden no ser suficientes para hacer frente a amenazas de malware y ransomware.

Estoy preocupado porque las medidas de protección de datos existentes en mi organización no sean suficientes para hacer frente a las amenazas de malware y ransomware

2022 **67 %** → **2023** (solo ITDM) **75 %**

Resumen: Combinación de "Totalmente de acuerdo" y "De acuerdo"

Políticas de ransomware

En una era en la que las amenazas cibernéticas representan una amenaza siempre presente, las políticas de seguro pueden proporcionar a las organizaciones seguridad. Sin embargo, a pesar de que las políticas de ransomware son comunes (93 %), siguen siendo escasas:

57 % Mi organización debe probar las "prácticas recomendadas" de actividad de prevención de ciberataques

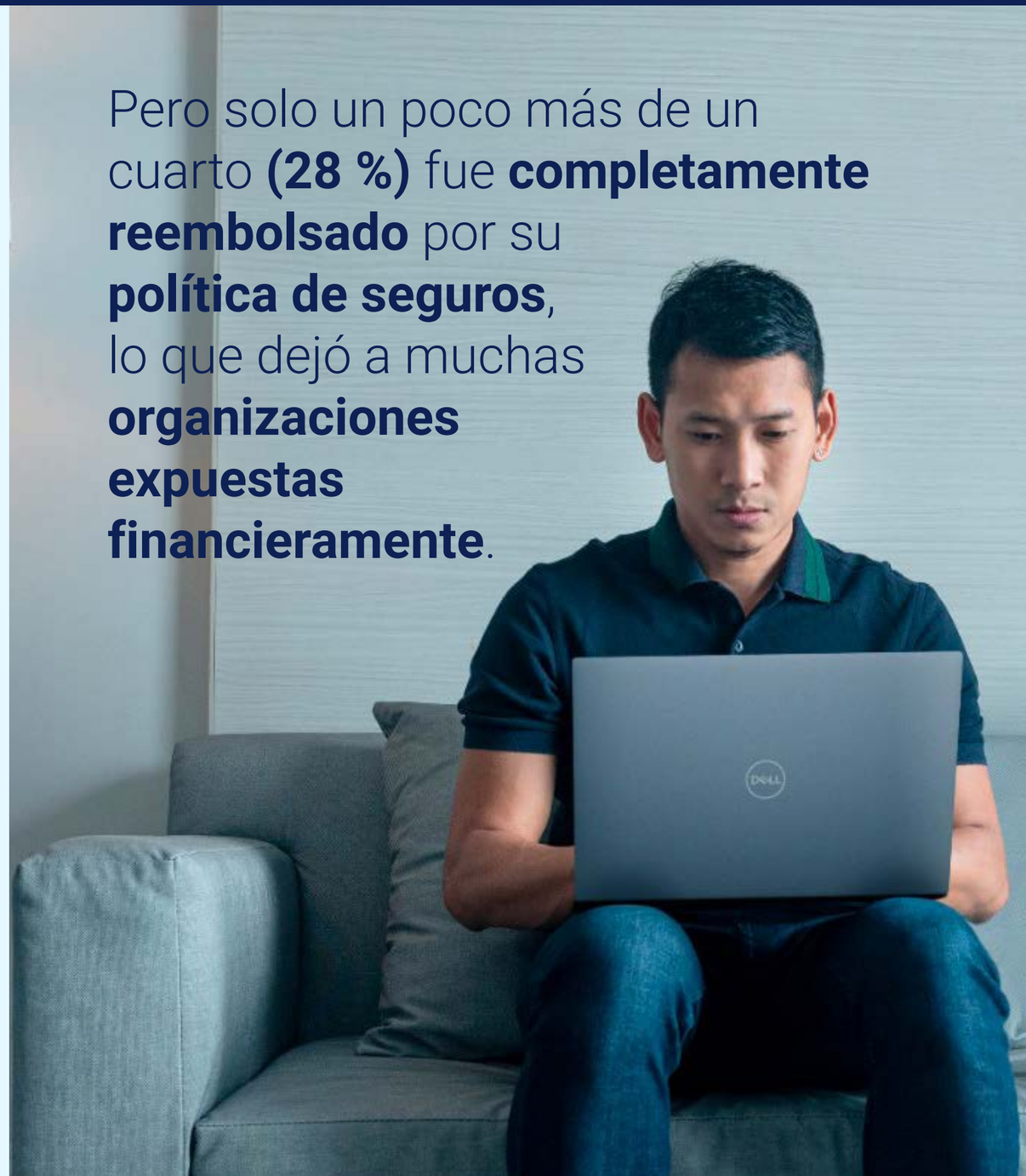
43 % La política tiene un límite en cuanto a cuánto pagarán por un reclamo

40 % Existen escenarios particulares que anularían la política

40 % La política no pagará, ya que el pago a algunas entidades puede estar restringido por la ley

85 % Para aquellos que experimentaron un ataque de ransomware, la gran mayoría pagó para acceder a sus datos.

Pero solo un poco más de un cuarto **(28 %)** fue **completamente reembolsado** por su **política de seguros**, lo que dejó a muchas **organizaciones expuestas financieramente**.



IA generativa y ciberseguridad

A medida que se expande el panorama de las amenazas cibernéticas, está emergiendo un cambio significativo hacia la adopción de la IA generativa como una herramienta estratégica para reforzar las defensas cibernéticas.

52 % se cree que la integración de la IA generativa proporcionará una ventaja a la postura de seguridad cibernética de su organización en la batalla continua contra los cibercriminales.

Sin embargo, este optimismo se vería afectado por el reconocimiento de los desafíos inherentes.

88 %

de los expertos coinciden en que adoptar la IA generativa generará grandes volúmenes de datos nuevos, lo que requerirá medidas de protección y seguridad.

Del mismo modo,

88 %

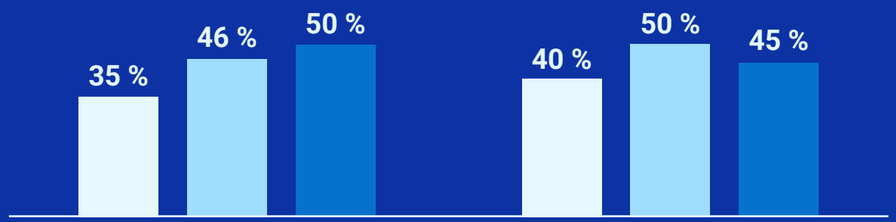
está de acuerdo en que la IA generativa amplificará el valor de tipos de datos específicos y, por lo tanto, exigirá niveles elevados de servicios de protección de datos.

Esta información valiosa destaca la naturaleza doble de la IA generativa como un recurso defensivo potente y una fuente de nuevas complejidades de ciberseguridad.

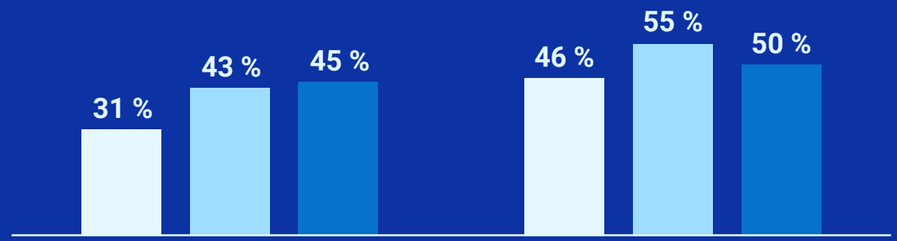
El uso de las múltiples nubes

La adopción de soluciones de nube pública sigue siendo una estrategia preferida para las organizaciones que buscan implementar o actualizar aplicaciones. Sin embargo, esta preferencia también introduce una capa adicional de complejidad de la protección de datos.

Implementación de aplicaciones nuevas



Actualización de aplicaciones existentes



96 % de las organizaciones se enfrentan a desafíos en la administración de datos dentro de entornos públicos de múltiples nubes.

44 % lidia con las complejidades inherentes a la navegación por varias plataformas de nube pública, cada una con sus características y requisitos únicos.

40 % expresa inquietudes sobre la protección de sus datos en estos diversos entornos.

Protección de un entorno de múltiples nubes

Con el aumento de las amenazas cibernéticas, muchas organizaciones no confían en mantener sus datos seguros en la nube, especialmente cuando implementan nuevas aplicaciones y actualizan las existentes. De hecho, la confianza está en un nivel bajo en todo momento.

Porcentaje de encuestados que no están "muy seguros" de la capacidad de su organización de proteger todos sus datos en entornos de nube pública

De manera comprensible, más de la mitad de los encuestados prioriza dos funcionalidades como fundamentales para permitir operaciones híbridas y de múltiples nubes eficaces:

58 %

La capacidad de proteger entornos de cargas de trabajo múltiples

56 %

Garantía de una ciberseguridad sólida

50 %

Para abordar estos desafíos, la mitad de las organizaciones ya ha traído soporte externo para mejorar la resiliencia cibernética.

Conclusión

A medida que las organizaciones recurren cada vez más a soluciones de nube pública, implementan modelos de trabajo híbridos y experimentan con la IA generativa, la criticidad de la protección de datos es más evidente que nunca. Sin embargo, asegurar y proteger los recursos digitales se está convirtiendo en un reto más complejo para muchos. En un panorama continuamente amenazado por los ataques cibernéticos, es esencial que las empresas adopten medidas que refuercen la resiliencia de sus operaciones.

Obtenga más información sobre la protección de datos de múltiples nubes moderna, simple y resistente de Dell: **www.dell.com/dataprotection**

DELL Technologies

Dell Technologies ofrece recuperación cibernética, respaldo, recuperación ante desastres, retención a largo plazo y más para ayudarlo a proteger todos sus datos y aplicaciones.

VansonBourne

Vanson Bourne es un especialista independiente en investigación de mercado del sector de tecnología. Su reputación por la realización de análisis sólidos y creíbles centrados en la investigación se basa en principios rigurosos de investigación y en la capacidad de solicitar la opinión de tomadores de decisiones ejecutivos que ejercen funciones técnicas y de negocios en todos los sectores comerciales y todos los mercados principales. **www.vansonbourne.com**