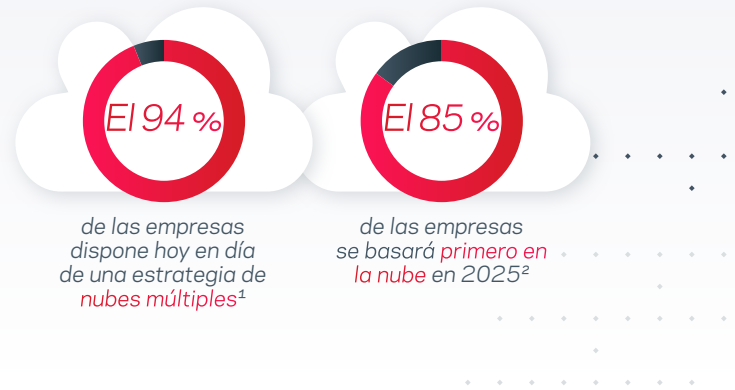


## Administración de los puntos problemáticos de la nube

### Las estrategias en la nube son complicadas.

A medida que las empresas trasladan sus recursos a la nube, muchas de ellas se percatan de que un almacenamiento mal administrado puede generar costes importantes. Si bien la nube aporta muchas ventajas, también plantea retos nuevos en ámbitos tan esenciales como la seguridad, la incertidumbre, los costes y la complejidad.



### Reto n.º 1

## La ciberseguridad es difícil

En 2021, el ransomware costó a las empresas

20 000 millones de USD



El ransomware y otras modalidades de software malicioso no solo son un problema muy grande, sino que también están empeorando.

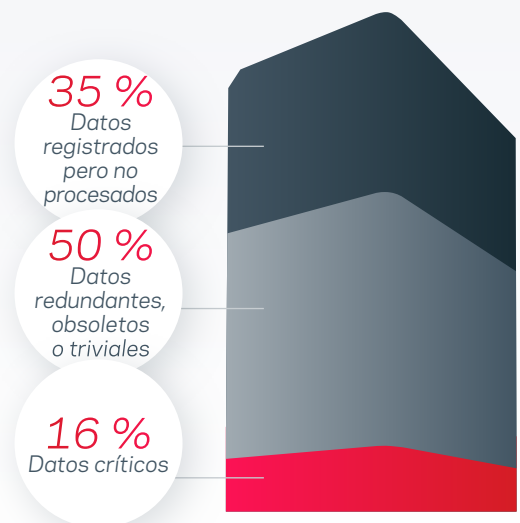
- Solo en la primera mitad de 2022, se han producido 2800 millones de ataques de software malicioso. Esto representa un incremento del 11 % respecto a los seis meses anteriores.<sup>3</sup> ¿Resultado? Las vulnerabilidades y los costes también aumentan de manera exponencial.
- En 2021, el coste promedio de un ataque fue de 1,85 millones de dólares.<sup>4</sup>
- Veritas descubrió que el 77 % de los negocios y las principales empresas de TI se ha sorprendido de la gran cantidad de recursos que dedicaron a las herramientas de ciberseguridad y la administración de datos.<sup>1</sup>
- Los errores de ciberseguridad son caros y pueden comportar la pérdida de ingresos, multas, sanciones legales y daños en la reputación de la marca.

## Reto n.º 2

### La incertidumbre, los datos registrados pero no procesados y la falta de visibilidad son peligrosos

*La visibilidad de los datos, desde el perímetro y el núcleo hasta la nube, es esencial para la resiliencia y la protección de los datos.*

- La mayoría de los responsables de TI es incapaz de realizar el seguimiento del espacio de los datos de toda la empresa, lo que dificulta aún más la protección de los datos, la detección de posibles amenazas como el software malicioso, así como la optimización de los costes y la complejidad.
- Según la investigación efectuada por Veritas, las personas encuestadas indicaron la falta de claridad de sus datos. De promedio, tienen un 35 % de datos registrados pero no procesados, un 50 % de redundantes, obsoletos o triviales, y solo un 16 % de datos empresariales críticos.<sup>5</sup>



## Reto n.º 3

### Los costes se pueden disparar



*Debido a un incremento de los requisitos de almacenamiento que es difícil de asumir, los costes se incrementan muchísimo.*

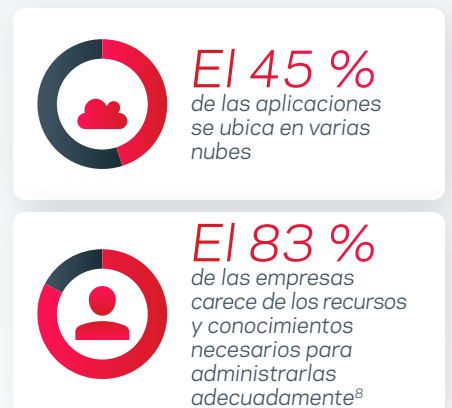
- Las soluciones antiguas de almacenamiento de datos no optimizan el uso, lo que genera datos duplicados e innecesarios que se acumulan en varias ubicaciones.
- En los últimos años, los costes de almacenamiento de datos no han dejado de crecer. McKinsey & Co. indica que en los cinco últimos años han aumentado un 50 %.<sup>6</sup>
- Desduplicar los datos, comprimirlos y después almacenarlos en un nivel más económico permite que las empresas ahorren hasta un 99 % en comparación con las instantáneas nativas de la nube.<sup>7</sup>

## Reto n.º 4

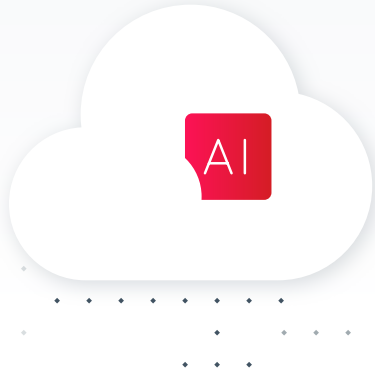
### La complejidad se convierte en la opción predeterminada

*Una acumulación de herramientas, tecnologías y recursos introduce capas adicionales de administración de TI en silos.*

- Las herramientas basadas en la nube se pueden activar enseguida; sin embargo, no pueden administrar infraestructuras distribuidas en varias nubes, lo que incrementa el uso de herramientas diferentes y la complejidad operativa.
- A fin de controlar la complejidad, las empresas deben adoptar soluciones que asuman y agilicen la administración unificada de datos complejos, mejoren la seguridad y la protección de los datos, y permitan una arquitectura basada en la nube que sea elástica y escalable.



### La nube aún necesita mucha supervisión manual



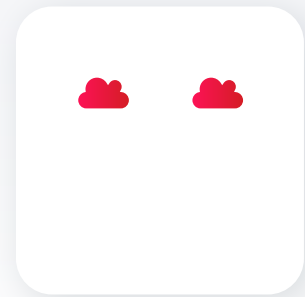
La automatización es imprescindible para eliminar los costosos errores comunes y manuales. Su valor es especialmente aparente en casos prácticos relacionados con:

- La tecnología de administración de datos autónomos que, de forma automática e inteligente, protege los datos, a la vez que asegura su cumplimiento, es segura y optimiza los costes.
- La inteligencia artificial, el aprendizaje automático y otras funciones de automatización y escala automática que admiten una arquitectura basada en la nube elástica y escalable.
- Los dispositivos, contenedores y microservicios que maximizan las prestaciones de las arquitecturas nativas de la nube.

### Confusión sobre el modelo de responsabilidad compartida.

Entre los proveedores de servicios en la nube y sus clientes, existe una confusión y una ambigüedad considerables respecto al modelo de responsabilidad compartida. En teoría, muchos entienden que los proveedores de servicios en la nube son los responsables de la resiliencia de la nube y que el cliente es responsable de la responsable de resiliencia en la nube. Ahora bien, la ejecución de estas responsabilidades sigue siendo vaga; a menudo, los datos y las aplicaciones se quedan sin protección y son vulnerables.

Con una plataforma sofisticada compatible con los entornos modernos de nubes múltiples, Veritas posibilita un mayor control, la reducción de riesgos y costes y, al mismo tiempo, asegura que pueda cumplir su parte del modelo de responsabilidad compartida.



## Veritas lo cambia todo

Veritas ofrece tecnología de próxima generación que revoluciona la administración y la resiliencia de los datos, la ciberseguridad y la sostenibilidad en la nube.

Más información en [www.veritas.com/es/es/solution/cloud-data-security](http://www.veritas.com/es/es/solution/cloud-data-security)

**VERITAS™**

+1 (866) 837 4827  
2625 Augustine Drive, Santa Clara,  
CA 95054, EE. UU.

[www.veritas.com](http://www.veritas.com)  
Para obtener información de contacto global,  
visite: [veritas.com/company/contact](http://veritas.com/company/contact)

1. Veritas and Vanson Bourne, "The Vulnerability Lag." [https://www.veritas.com/content/dam/Veritas/docs/reports/GA\\_ENT\\_AR\\_Veritas-Vulnerability-Gap-Report-Global\\_V1414.pdf](https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf)  
2. Gartner, "Gartner Identifies Four Trends Driving Near-Term Artificial Intelligence Innovation," 7 de septiembre de 2021. <https://www.gartner.com/en/newsroom/press-releases/2021-09-07-gartner-identifies-four-trends-driving-near-term-artificial-intelligence-innovation>  
3. SonicWall, "2022 Cyber Threat Report." <https://www.sonicwall.com/2022-cyber-threat-report/>  
4. Cloudwards, "Ransomware Statistics, Trends and Facts for 2022 and Beyond," 22 de marzo de 2022. <https://www.cloudwards.net/ransomware-statistics/>  
5. Veritas and Vanson Bourne, "The Vulnerability Lag." [https://www.veritas.com/content/dam/Veritas/docs/reports/GA\\_ENT\\_AR\\_Veritas-Vulnerability-Gap-Report-Global\\_V1414.pdf](https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf)  
6. McKinsey, "Reducing data costs without jeopardizing growth", 31 de julio de 2020. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/reducing-data-costs-without-jeopardizing-growth>  
7. Veritas, "Cloud-Optimized Backup from Snapshot and Autoscaling in NetBackup 10." [https://www.veritas.com/content/dam/www/en\\_us/documents/technical-documents/TB\\_netbackup\\_cloud\\_optimized\\_backup\\_snapshot\\_V1510.pdf](https://www.veritas.com/content/dam/www/en_us/documents/technical-documents/TB_netbackup_cloud_optimized_backup_snapshot_V1510.pdf)