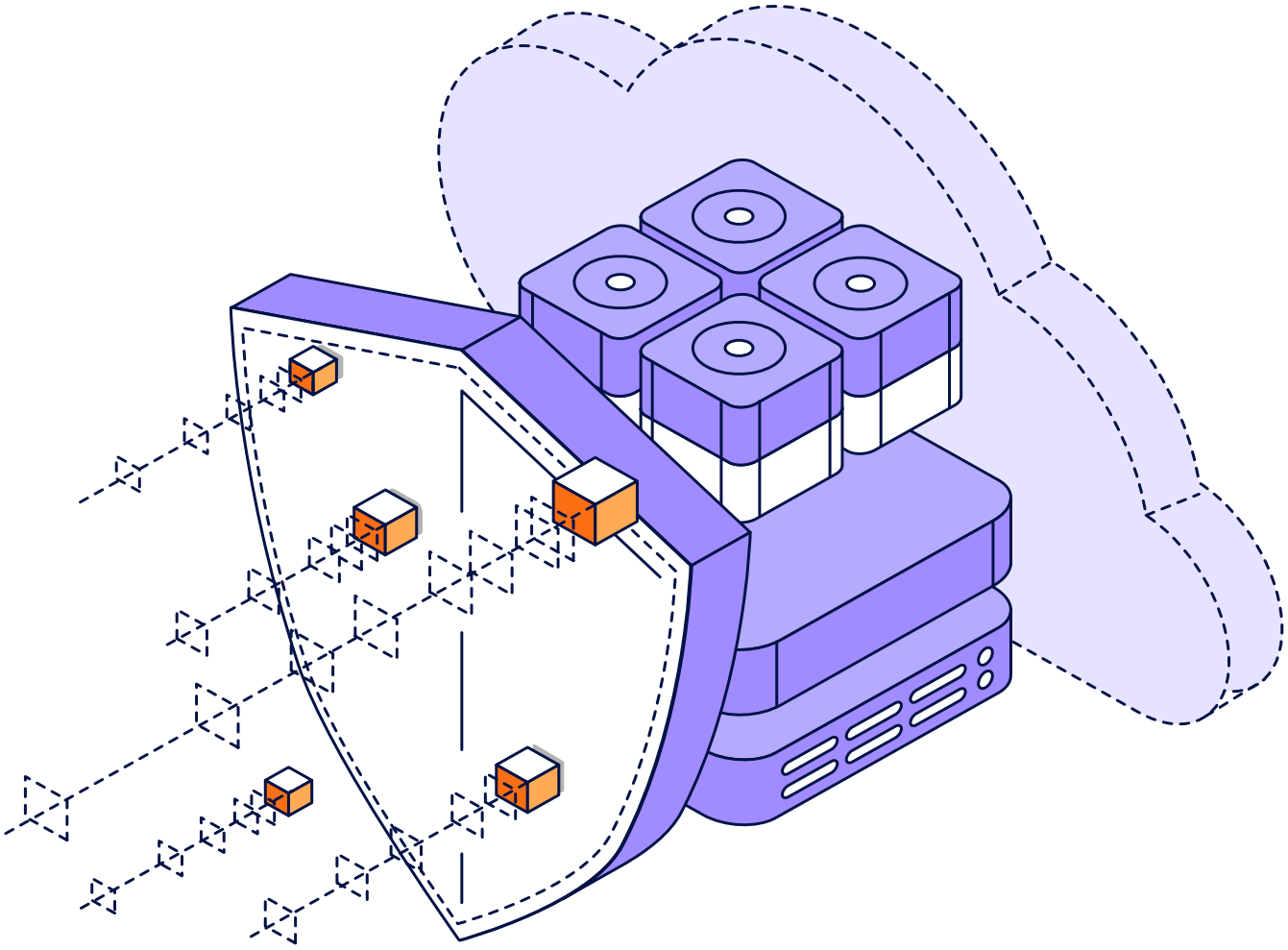
Ciberresiliencia para la nube híbrida

Lecciones aprendidas de más de 7000 profesionales de TI y seguridad



En los últimos años hemos pasado de los centros de datos locales (on-premises) a la nube "***cuando tiene sentido", a las estrategias en las que se daba*** prioridad a los entornos ***cloud***, pasando por *un enfoque* ***híbrido en todos sitios, para terminar en la situación actual, en la*** que la mayoría de las organizaciones aplican una "***estrategia multicloud" como la forma habitual de prestación de sus servicios*** de TI. En 2024, las dudas no giran en torno a si aplicar o no servicios basados en la nube, ni tampoco sobre qué servicios cloud usar. Al contrario, la pregunta que asalta a las organizaciones es la de cuántas nubes son necesarias y de qué forma podrán gestionar los equipos de TI todas las nubes para garantizar al mismo tiempo la capacidad de responder frente a problemas de ciberseguridad, contar con una estrategia de protección de datos sólida y disponer de otros controles de TI críticos.

Para dar respuesta a todas estas preguntas, este informe recopila tres fuentes de investigación independientes que fueron analizadas entre agosto de 2022 y marzo de 2023, en el que se incluye:

- **Tendencias de protección en la nube para 2023**
  Estudio con 1700 administradores de IaaS, PaaS y SaaS sobre sus estrategias de protección de datos.
- **Informe de tendencias de protección de datos 2023**
  Un sondeo realizado con 4200 profesionales de TI responsables de las estrategias de protección de datos de sus respectivas organizaciones.
- **Informe de tendencias de ransomware 2023**
  Estudio en el que participaron 1200 profesionales CISO/SecPro/Backup cuyas organizaciones sufrieron un ciberataque en algún momento de 2022.

Estos tres estudios fueron llevados a cabo por agencias de investigación o análisis independientes y comités imparciales, cuyos datos posteriormente fueron adquiridos y publicados de diversas formas por Veeam®. En este informe, se ponen de relieve claramente cuatro áreas clave:

- Los servicios basados en la nube son fundamentales para proteger los centros de datos y las cargas de trabajo alojadas en la nube.
- Las nubes son igual de susceptibles de sufrir un ataque de ransomware, quizá incluso más.
- Usar una nube para proteger otra es una buena idea; pero usar la misma nube para protegerse a sí misma no lo es tanto.
- Los equipos de seguridad, de DR, cloud y on-prem no están alineados; esto es lo primero que hay que solucionar.

Los servicios basados en la nube son fundamentales para proteger los centros de datos y las cargas de trabajo alojadas en la nube.

El 82 %
de las organizaciones ahora usan almacenamiento basado en la nube que puede ser inmutable.

El estudio demuestra de manera fehaciente que los servicios basados en la nube constituyen un aspecto indispensable para proteger cargas de trabajo locales (on-premises) tradicionales, así como cargas de trabajo alojadas en la nube. *En especial, el almacenamiento basado en la nube permite disponer de* ***repositorios que "pueden sobrevivir"*** *(p. ej., que son inmutables), así como una* ***infraestructura de recuperación ante desastres*** *cuando lo necesite.*

Para la mayoría de las organizaciones, existen determinadas verdades que son prácticamente universales en referencia a la protección contra ransomware:

- Para proteger los servidores de los centros de datos, saque los datos del edificio (por ejemplo, a un sitio externo o a una nube).
- Para poder recuperarse tras un ataque de ransomware, necesitará copias de backup que no se hayan visto afectadas por las ciberamenazas.

Según el informe de tendencias del ransomware 2023, hay que tomar la combinación de ambos axiomas como una lección aprendida de 2023, ya que el **82 %** de las organizaciones aprovechan ahora almacenamiento cloud con capacidad para ser inmutable.[1]

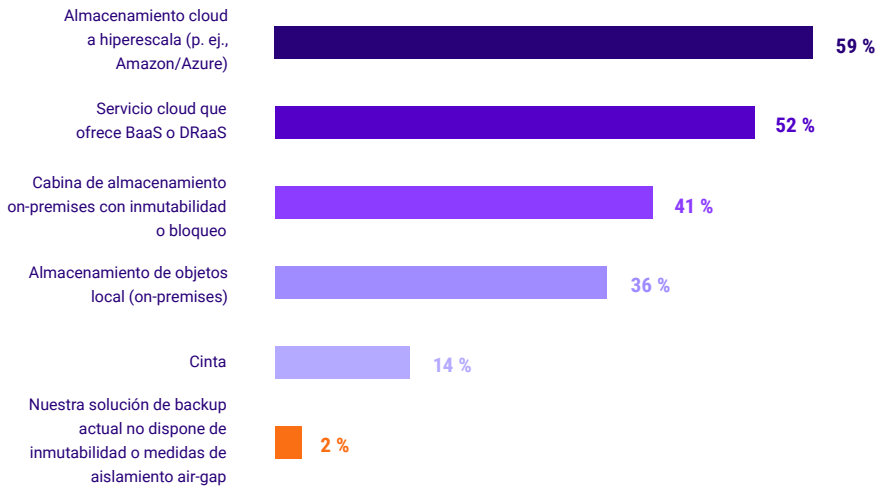


Figura 1.1

¿Utiliza su organización backups offline, aislados (air-gapped) o inmutables usando los siguientes sistemas?

Una vez que se ha garantizado que la organización dispone de copias de backup que pueden sobrevivir, se pueden considerar otros aspectos de una estrategia tradicional de continuidad de negocio o recuperación ante desastres (BC/DR). En el momento actual, en el que cada vez son más los que consideran los ciberataques como otra forma de desastre (aunque especial), no sorprende que muchos piensen que la ciberresiliencia y la recuperación ante catástrofes están muy interrelacionadas. En ambas situaciones, la pregunta más práctica que puede hacerse es: **"¿en dónde recuperará, o a qué ubicación va a hacer Failover".**

A modo de lección aprendida por las víctimas de ciberataques, las estrategias de recuperación de las organizaciones incluyen la posibilidad de recuperar los servidores de sus centros de datos a infraestructuras alojadas en la nube cuando se intenta recuperar de un ataque de ransomware u otro tipo de crisis.[2]

Figura 1.2

¿Al recuperar los servidores tras un ataque de ransomware, dónde recupera sus datos?

Los datos anteriores revelan que la mayoría de las organizaciones cuentan con una estrategia híbrida que es flexible y depende del alcance del desastre. De hecho, el **71 %** de las organizaciones puede recuperarse usando una nube, mientras que el **81 %** puede recuperarse utilizando una infraestructura local (on-premises) y esto supone un solapamiento importante (flexibilidad). Dentro del amplio rango de desastres para los que se preparan las organizaciones en base a sus planes de recuperación ante desastres, el **54 %** prevé hacer failover a una ubicación alternativa, mientras que el **46 %** prevé **usar la infraestructura alojada en la nube como su sitio de recuperación de desastres**. Una vez dicho esto, hay que decir que hay más de una forma de conseguir un sitio de recuperación ante desastres que esté basado en la nube.[3]

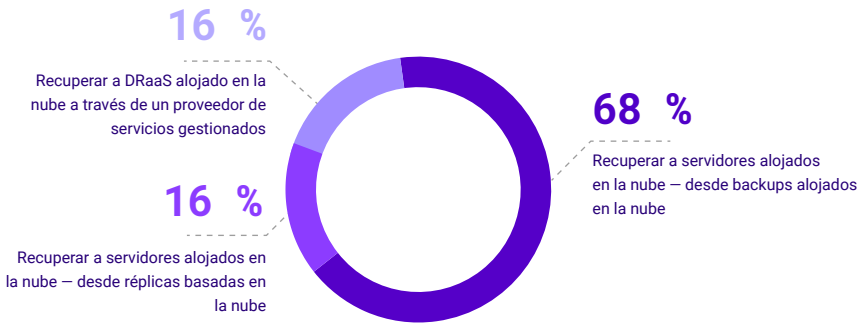


Figura 1.3

¿Al usar servicios cloud para la recuperación ante desastres, cómo se reanudan las operaciones?

Tanto si su plan de recuperación ante desastres aprovecha los servicios de un proveedor de Disaster Recovery as-a-Service (DRaaS), como una infraestructura gestionada por uno mismo alojada en la nube como Amazon Web Services o Microsoft Azure, existen finalmente dos funcionalidades críticas para tener éxito

- La capacidad de transformar un backup durante la restauración, de forma que un servidor protegido pueda recuperarse y ejecutarse en un host alojado en la nube, con independencia de que en origen fuera físico o virtual.
- La capacidad de orquestar todo el proceso de recuperación, incluido el aislamiento en cuarentena para la detección de malware durante el flujo de trabajo de restauración.

Desafortunadamente, sólo

- **el 18 %** de las organizaciones son capaces de programar flujos de trabajo orquestados para la recuperación mediante failover.[4]
- **El 44 %** utiliza un área de pruebas aislada o "sandbox" para buscar malware durante la restauración, como parte de la estrategia para evitar la reinfección del entorno.[5]

La dirección debería abordar cuestiones complejas tales como si la solución o servicio de protección de datos de su organización puede automatizar la recuperación a gran escala y garantizar una restauración segura.

Las nubes son igualmente susceptibles de sufrir un ataque de ransomware, quizá incluso más.

El estudio revela de manera sistemática que las cargas de trabajo basadas en la nube tienen las mismas probabilidades de verse afectadas durante un ciberataque, y el motivo presumiblemente sea que *estos servicios cloud son perfectamente accesibles dentro de las arquitecturas híbridas de TI, De hecho, si se tiene en cuenta que muchas organizaciones deben utilizar diferentes tecnologías de seguridad para impedir el acceso a los servicios en la nube frente a los recursos de sus centros de datos, afloran oportunidades de ataque adicionales, como la interrupción de la conexión entre los usuarios y sus plataformas en la nube.*

De la misma forma que entendemos que la "nube no está llegando, ya está aquí", hay que reconocer también que los departamentos de TI no están retirando las plataformas locales al mismo ritmo con el que se da la bienvenida a nuevas cargas de trabajo en servicios basados en la nube. Las organizaciones siguen adoptando la infraestructura alojada en la nube como parte de una estrategia cada vez más híbrida para la prestación de los servicios de TI.

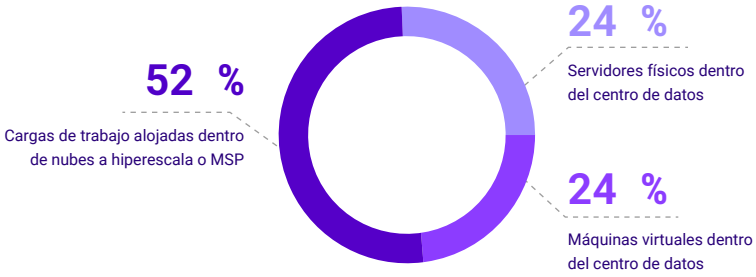


Figura 2.1

Distribución "híbrida" de plataformas prevista para cargas de trabajo del servidor de producción en 2024.[6]

A diferencia de la evolución vista en las plataformas informáticas basada en el centro de datos, cabe decir que no existe una única arquitectura de "nube" que se despliegue, utilice y proteja: independientemente del proveedor de la nube. Por el contrario, hay que considerar que existe una infinidad de arquitecturas de nube, cada una de ellas provenientes de distintos proveedores cuyos marcos de gestión subyacentes varían drásticamente entre ellos.

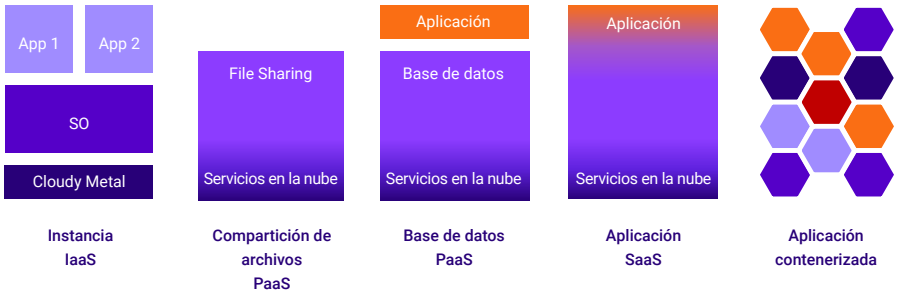


Figura 2.2

Multitud de arquitecturas cloud.

Desafortunadamente, pese a que normalmente se tiene la percepción de que los servicios basados en la nube son resilientes de por sí, siguen produciéndose interrupciones provocadas por problemas achacables al proveedor de servicios cloud, a errores de configuración de los servicios en la nube por parte de los administradores, y a la conectividad entre los usuarios y los propios servicios cloud. Dicho esto, tanto en el informe de 2021 como en el de 2022, las interrupciones debidas a ciberataques aumentaron interanualmente, y siguieron siendo la causa de interrupción con un mayor impacto, tanto en 2021 como en 2022 (y no hay signos de que esta tendencia vaya a disminuir en 2023).[7]

- **El 48 %** de las organizaciones sufrieron interrupciones en sus servicios de TI debido a que **"los recursos de la nube pública no estaban disponibles".**
- **El 52 %** de las organizaciones sufrieron la parada de los sistemas informáticos debido a **"interrupciones** de **la red o la infraestructura**.
- **El 53 %** de las organizaciones sufrieron interrupciones de sus sistemas informáticos debido a **"incidentes de ciberseguridad".**

Aunque la entrada inicial pueda ser sistemáticamente oportunista (por ejemplo, enviar correos electrónicos de phishing y esperar que un usuario haga clic), en la mayoría de los ciberataques, esos mismos atacantes apuntan posteriormente a los sistemas en busca de vulnerabilidades conocidas o posibles insuficiencias en la adecuada protección de las plataformas de TI más populares. El estudio del Informe de tendencias de ransomware 2023 muestra que, en el **38 %** de los ataques, el **objetivo de los ciberdelincuentes eran las cargas de trabajo alojadas en la nube.** [8]

Tras preguntar a 1200 víctimas de ciberataques se descubrió que estos ciberataques cifraron o afectaron prácticamente al mismo volumen de datos en la nube y en el centro de datos.

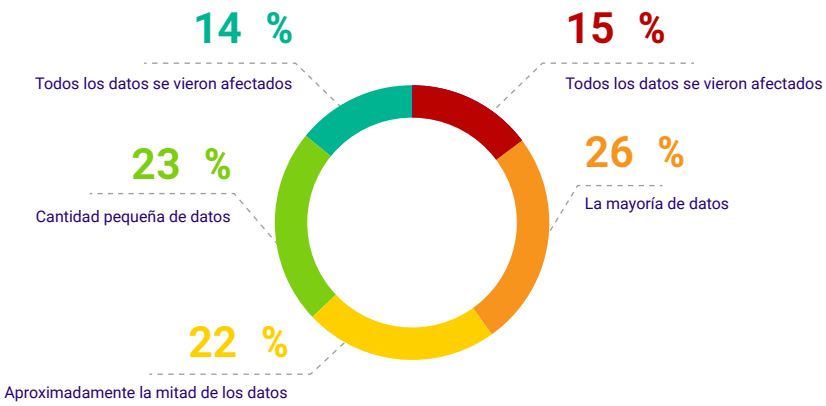


Figura 2.3

% de datos alojados en plataformas cloud que se vieron afectados por el último ataque de ransomware.[9]

Es importante destacar que las similitudes en las tasas de infección entre los datos del centro de datos, de las sucursales/oficinas remotas y de los datos alojados en la nube infieren dos realidades clave:

- Dado que la TI híbrida trabaja de una forma fluida y sin barreras, una vez que una ciberamenaza opera en el entorno de la víctima, los datos alojados en la nube son tan vulnerables a sufrir los ataques como las aplicaciones y archivos del centro de datos físico.
- Debido a esa fluidez y similitud en materia de vulnerabilidad, los archivos, bases de datos y aplicaciones alojados en la nube deben protegerse con la misma rigurosidad y metodologías que las cargas de trabajo locales.

Para 2024, se espera, por primera vez, que se ejecuten más cargas de trabajo fuera de los centros de datos físicos autogestionados que en los entornos locales de siempre.

Usar una nube para proteger otra es una buena idea; pero usar la misma nube para protegerse a sí misma no lo es tanto.

2 : 1

la mayor parte de las tareas de protección de datos la realiza el equipo de backup de TI tradicional, comparado con los administradores cloud.

Cuando se preguntó sobre "quién" hacía el backup de los datos en la nube y "cómo" se protegían los datos en 2023, los tres estudios confirmaron que ***el equipo "central" de backup (o el proveedor de servicios) que protege el resto de datos locales de una organización, se encarga frecuentemente también de proteger los datos*** *alojados en la nube. Dicho esto, existe todavía mucha confusión sobre el "cómo" se protegen los datos, y es algo típico que las organizaciones asuman que su única opción es usar la utilidad "integrada" en la plataforma, en vez de una solución heterogénea de backup empresarial.*

Antes de considerar "cómo" protegen las organizaciones las cargas de trabajo alojadas en la nube, es importante considerar las opciones para el "quiénes" las protegen. De manera relativamente constante, los responsables de la protección de estos datos son los equipos de backup tradicional frente a los administradores cloud, en una relación de dos a uno.

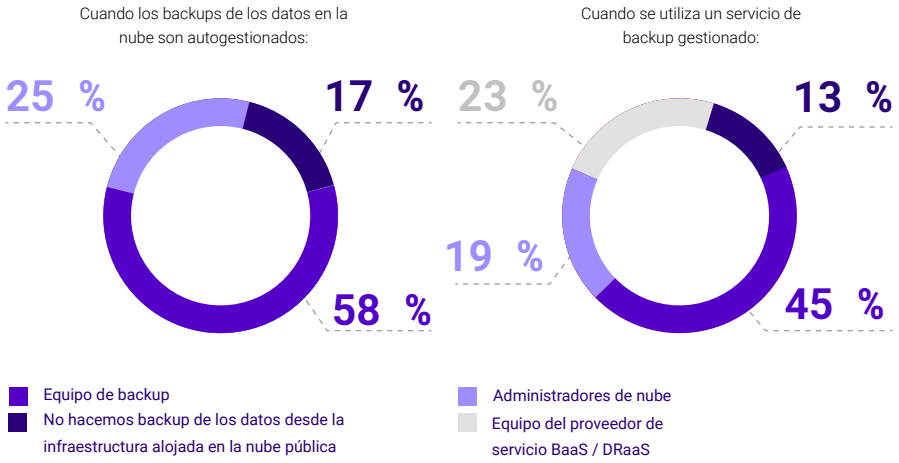


Figure 2.1

¿Quién de su organización administra los backups y la protección de los servidores alojados en la nube?[10]

Sorprendentemente, uno de cada ocho **(13 %)** cree que sus organizaciones no realizan el backup de su infraestructura alojada en la nube. Seguidamente, la siguiente cuestión a considerar por muchas de las organizaciones que adoptan estrategias híbridas es el reconocimiento de que los backups de la nube podrían residir en la misma nube, en una región distinta, una nube diferente o incluso de nuevo en las instalaciones locales.
Esta cuestión es importante a la hora de elegir una solución de backup para las cargas de trabajo alojadas en la nube:

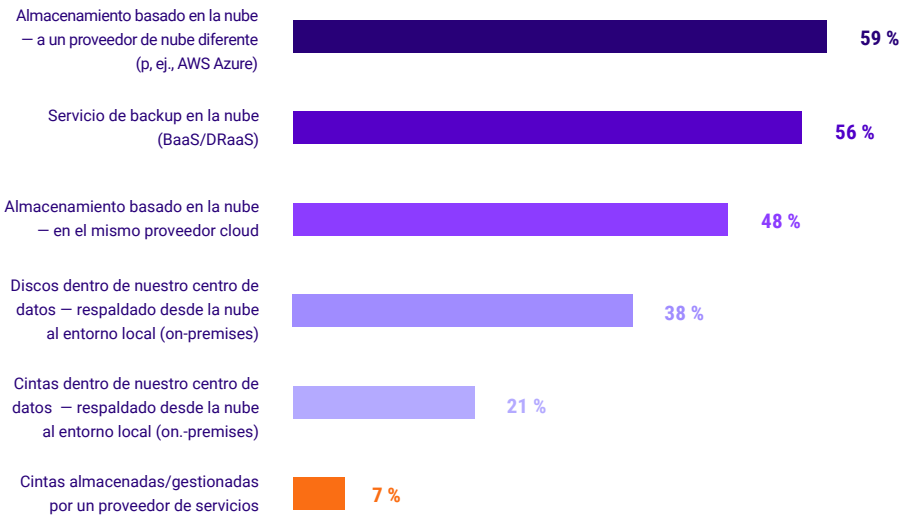


Figura 3.2

¿Para los datos de backup en la nube que retiene su organización durante un año o más, dónde se almacenan esos backups?[11]

- **El 37%** de los responsables de TI considera que "la posibilidad de trasladar cargas de trabajo de una nube a otra" es un aspecto determinante de una solución de protección de datos "moderna" o "innovadora".[12]
- El **88 %** de las organizaciones ha movido cargas de trabajo de la nube a las instalaciones locales o a otra nube.[13]

Obviamente, la otra opción que existe a la hora de elegir una solución de backup para las cargas de trabajo que se alojan en la nube es confiar sencillamente en la utilidad o función de exportación "integrada" que muchas empresas cloud ofrecen para cada carga de trabajo particular. En muchas ocasiones, el factor que limita las opciones es el simple conocimiento de que existen herramientas de terceros que protegen de forma completa las cargas de trabajo en la nube.[14]

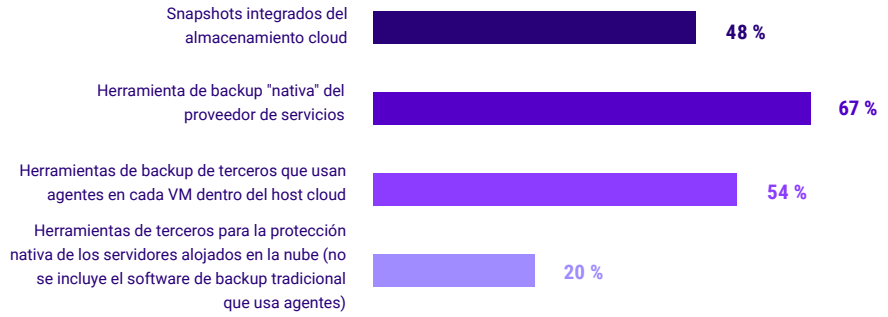


Figura 3.3

¿Qué mecanismos de protección de datos alojados en la nube conoce (con independencia de si los usa o no a día de hoy)?

*Si se considera el uso de snapshots, pregúntese si confiaría estrictamente en los snapshots de sus servidores de archivo locales.*Los snapshots son potentes herramientas de recuperación para puntos de recuperación muy cercanos al momento actual y que pueden ejecutarse al instante. Pero los **snapshots nunca han sido un sustituto de los backups por** los siguientes motivos:

- Presentan el mismo silo de exposición (se relaciona una NAS independiente con una pila de almacenamiento IaaS, incluyendo credenciales comunes).
- Son caros de conservar a lo largo del tiempo; por este motivo la mayoría de organizaciones conservan snapshots de unos pocos días, pero backups de semanas, meses y años.

Si se consideran utilidades "nativas" centradas en la carga de trabajo o integradas, pregúntese si sus plataformas locales están protegidas:

- Dependiendo solamente de ZDLRA (o RMAN) para la protección de bases de datos de **Oracle**.
- Dependiendo solamente de NT Backup Utility (o la herramienta del sistema) para hacer backup de los **Windows Servers**.
- Dependiendo solamente de VDPA para hacer backup de los hosts **VMware**.
- Dependiendo solamente de ASB para hacer backup de **Microsoft 365**.

Ahora pregúntese, cuántas herramientas quiere gestionar su equipo de TI para hacer backup y qué presupuesto tiene para almacenamiento (puesto que cada una de estas herramientas guarda en repositorios y formatos diferentes). La captura de snapshots y otras utilidades individuales de la plataforma (es decir las utilidades integradas) son si cabe más problemáticas si se considera que están diseñadas con un rango de retención limitado para permitir realizar restauraciones rápidas como consecuencia de un error reciente, como una sobreescritura o una importación errónea. Cuando se considera cómo se recuperará la organización tras un ataque de ransomware que puede haber estado latente durante semanas, estos enfoques tácticos parecen insuficientes (o prohibitivos por coste). Estos puntos de vista se cuantifican en dos estadísticas adicionales:

- El **35 %** de los responsables de TI consideran la **"protección estandarizada del entorno local e IaaS/SaaS"** como un aspecto determinante de una solución de protección de datos 'moderna' o 'innovadora'.[15]
- El **42 %** de las organizaciones creen que la **"capacidad para proteger cargas de trabajo alojadas en la nube"** es un atributo imprescindible de las soluciones de protección de datos empresariales.[16] Este punto de vista fue la respuesta más común y más importante para 2023.

El 35 %

de los responsables de TI consideran la "protección estandarizada del entorno local e IaaS/SaaS" como un aspecto determinante de una solución de protección de datos 'moderna' o 'innovadora'.

Los equipos de seguridad, de DR, cloud y on-prem no están alineados; esto es lo primero que hay que solucionar.

Los tres proyectos de investigación encuestaron a una amplia variedad de personas que incluían directores de TI responsables de la protección de datos, CISOs y ejecutivos similares, profesionales de la seguridad, administradores de IaaS/PaaS/SaaS y operadores de backup. Los tres estudios revelaron que ningún equipo era el encargado en exclusiva de una responsabilidad principal; siempre había solapamientos en cuanto a su influencia y su responsabilidad. Los datos mostraron que los encuestados rara vez pensaban que existía una correcta alineación entre los distintos equipos en materia de requisitos de ***estrategia o*** la ***implementación/uso de las tecnologías.***

Aunque la mayor parte de las iniciativas de estudio se centraban en las tecnologías utilizadas o las razones/estrategias que determinan la elección de dichas tecnologías, los datos de la encuesta revelan también una clara y constante falta de alineación entre las distintas personas involucradas en todas estas actividades.[17]

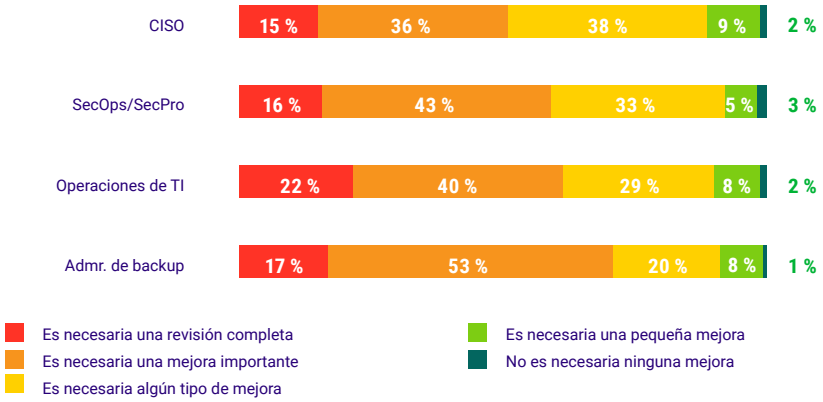


Figura 4.1

¿Cuánta mejora cree que es necesaria para que los equipos de backup informático de su organización y los de ciberseguridad estén completamente alineados?

Es importante recalcar que de los cuatro tipos de responsables encuestados en el informe de tendencias de Ransomware 2023, cuanto más "cerca" de las tareas de remediación del incidente se encontraba el profesional (por ejemplo, el administrador de backup frente al CISO), menos satisfecho estaba con la colaboración y la alineación entre los diferentes equipos.

Se observaron desajustes similares entre los administradores de SaaS y de backup al considerar el fundamento y las herramientas para la protección de Microsoft 365, e igualmente entre los administradores de IaaS/PaaS y los administradores de backup, cuando se consideran las estrategias y herramientas para proteger los servidores alojados en la nube, archivos compartidos y bases de datos.

¡Cuestiones a tener en cuenta!

En base a un estudio realizado con más de 7.000 encuestados durante un período de ocho meses, estas son algunas de las preguntas clave a considerar dentro de su estrategia de ciberresiliencia.

- ¿Son nuestros backups inmutables y están alojados en una ubicación externa? ¿Los backups los gestiona un proveedor experimentado o los gestionamos nosotros mismos?
- ¿Podríamos usar la infraestructura cloud como sitio de recuperación ante desastres? En caso negativo, ¿por qué no?
- ¿Hacemos backup de todos nuestros datos alojados en la nube, incluidas las cargas de trabajo de IaaS, PaaS y SaaS? En caso afirmativo, ¿usamos herramientas independientes para cada una de las nubes o las desplegamos de forma coherente para todas nuestras nubes (y cargas de trabajo locales)?
- ¿Hasta qué punto están alineados nuestros equipos con respecto al backup local, IaaS, PaaS y SaaS?
- ¿Hasta qué punto están alineados nuestros equipos entre la ciberpreparación y el backup de datos?
- ¿Cuándo fue la última vez que se probó la recuperación de nuestros datos alojados en la nube?
- ¿Cuándo fue la última vez que se probó la recuperación de un centro de datos a gran escala?
- ¿Cuándo fue la última vez que se evaluaron y actualizaron nuestros manuales de TI y BC/DR?

Si tiene cualquier pregunta sobre el informe o sus implicaciones, póngase en contacto con StrategicResearch@veeam.com.

Para leer los informes completos que aquí se mencionan, consulte los siguientes enlaces:

- **Tendencias de protección en la nube para 2023**
  Estudio con 1700 administradores de IaaS, PaaS y SaaS sobre sus estrategias de protección de datos.
- **Informe de tendencias de protección de datos 2023**
  Un sondeo realizado con 4200 profesionales de TI responsables de las estrategias de protección de datos de sus respectivas organizaciones
- **Informe de tendencias de ransomware 2023**
  Estudio en el que participaron 1200 profesionales CISO/SecPro/Backup cuyas organizaciones sufrieron un ciberataque en algún momento de 2022.

El punto de vista de Veeam

La plataforma de gestión de datos y backup de Veeam

Para las empresas es fundamental, ahora más que nunca, poder confiar en que sus datos estén siempre protegidos y disponibles, ya sea en las instalaciones locales como en el borde o en la nube. Veeam ofrece una plataforma única para entornos físicos, cloud, virtuales, SaaS y de Kubernetes. Nuestros clientes tienen la certeza de que sus aplicaciones y datos están protegidos contra el ransomware, desastres e individuos malintencionados, y siempre disponibles con la plataforma más sencilla, flexible, confiable y avanzada de la industria.

Veeam proporciona a los clientes la confianza para impulsar la Transformación Digital, protegerse de la ciberdelincuencia e impulsar la resiliencia del negocio, garantizando que sus datos estén siempre protegidos y disponibles. Reduzca el costo y la complejidad, y consiga los objetivos de su negocio con Veeam: la solución de backup y recuperación n.º 1.

Para obtener más información, visite **https://www.veeam.com/es**.

Para reunirse con un experto de Veeam en nube híbrida, haga su solicitud **http://vee.am/hybridcloudinquiry**.

Puede dirigir sus preguntas
sobre los datos e información
de este estudio directamente a
StrategicResearch@veeam.com

1 Informe de tendencias de ransomware 2023, Q29
2 Informe de tendencias de ransomware 2023, Q25
3 Informe de tendencias de protección de datos 2023, Q45
4 Informe de tendencias de protección de datos 2023, Q46
5 Informe de tendencias de ransomware 2023, Q21
6 Informe de tendencias de protección de datos 2023, Q2
7 Informe de tendencias de protección de datos 2023, Q13 y Q14
8 Informe de tendencias de ransomware 2023, Q9
9 Informe de tendencias de ransomware 2023, Q6
10 Tendencias de protección en la nube 2023, Q6
11 Tendencias de protección en la nube 2023, Q8
12 Tendencias de protección de datos 2023, Q17
13 Tendencias de protección en la nube 2023, Q4
14 Tendencias de protección de datos 2023, Q35
15 Tendencias de protección de datos 2023, Q17
16 Tendencias de protección en la nube 2023, Q4
17 Informe de tendencias de ransomware 2023, Q1