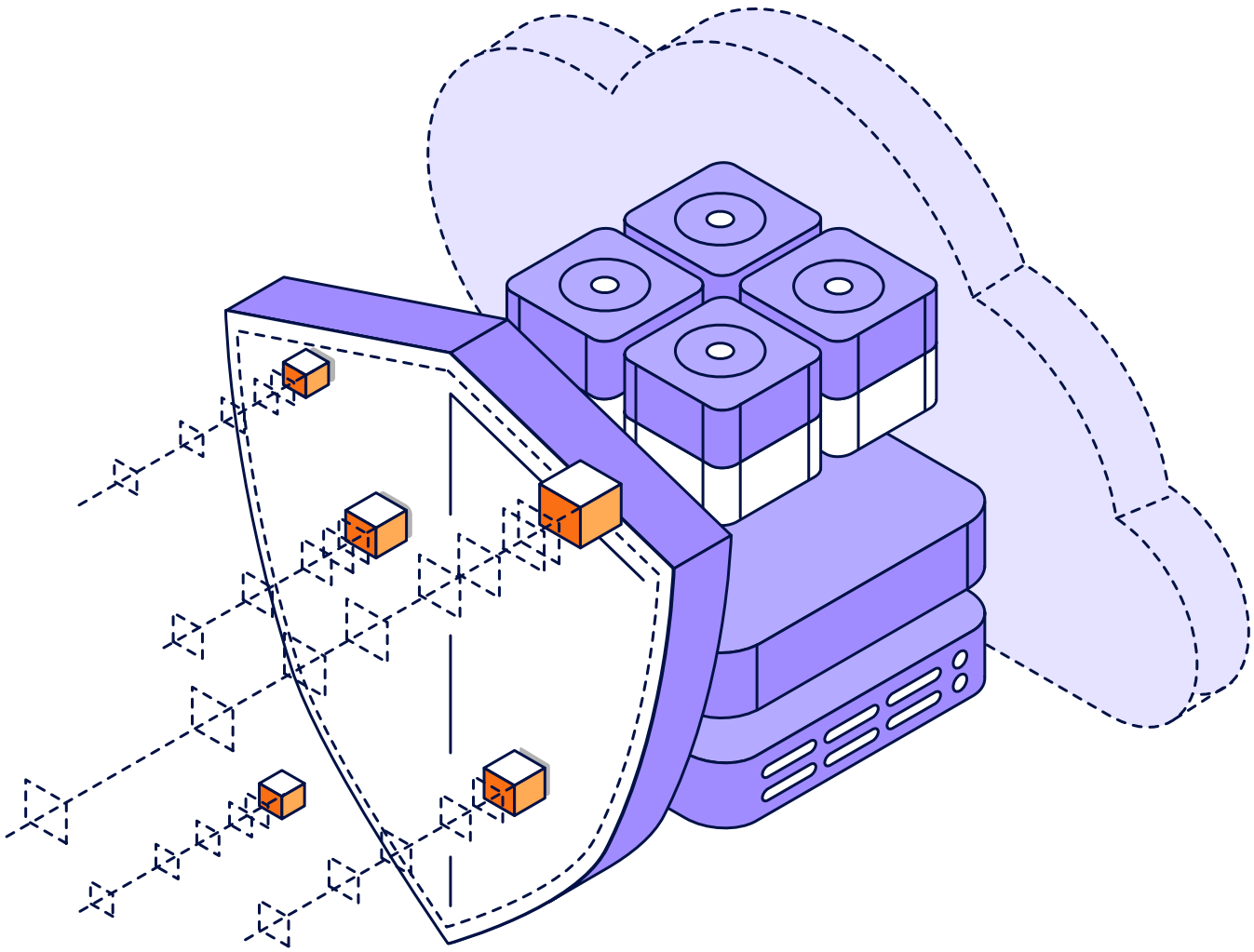
RESUMEN EJECUTIVO

Tendencias de protección en la nube para 2023

Edición para América



En el otoño de 2022, una firma de investigación independiente completó su encuesta a **1,700** líderes de TI imparciales con respecto a su uso de servicios en la nube en escenarios de producción y de protección, y se preguntó a personas representativas de cada escenario con el fin de que pudieran recopilarse todas las diferencias entre las perspectivas de las personas, así como los impulsores estratégicos y las metodologías de backup. De los **1,700** encuestados, **650** residían en el continente americano.

Este fue un estudio de mercado general sobre organizaciones imparciales que ejecutan al menos una carga de trabajo de producción en una nube (IaaS, PaaS o SaaS). La encuesta se realizó en nombre de Veeam con el fin de entender las perspectivas, responsabilidades y metodologías de las distintas personas en relación con la operación y la protección de las cargas de trabajo alojadas en la nube, así como las consideraciones al usar la protección de datos basada en la nube. El informe completo se encuentra en **http://vee.am/CPT23**.

TI híbrida = movimiento fluido hacia Y desde hosts en la nube

Para la mayoría de las organizaciones con una estrategia de "prioridad en la nube", las nuevas cargas de trabajo que pueden ejecutarse en una nube empezarán allí, mientras que solo menos de **1/3** de los servidores en la nube se iniciaron por primera vez en un host en la nube, y **2/3** se migraron desde el centro de datos. Dicho esto, el "viaje a la nube" no es unidireccional, ya que la mayoría de las organizaciones ha retirado cargas de trabajo de la nube en algún momento.

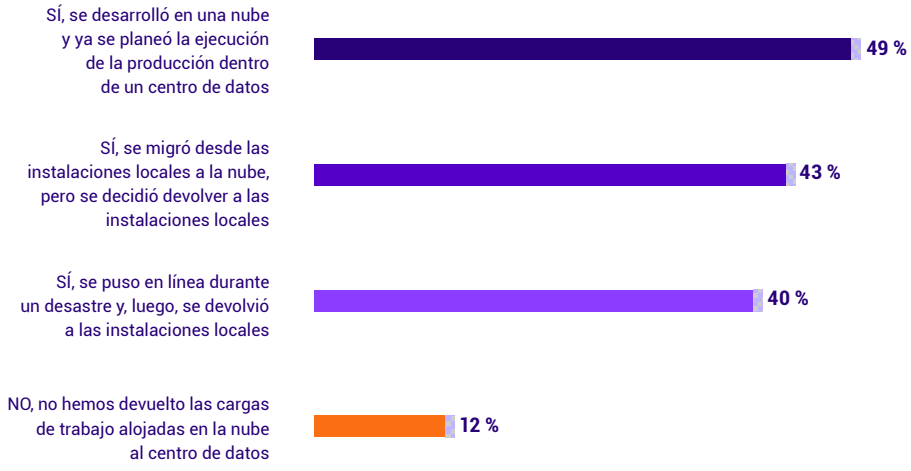


Figura 1.2

¿Su organización ha migrado de VUELTA alguna carga de trabajo de una nube pública a las instalaciones locales?

Cabe destacar que la fluidez de las cargas de trabajo que regresan a las instalaciones locales varía un poco según la región:

	INTERNACIONAL	América	EMEA	APJ
NO, no hemos devuelto las cargas de trabajo alojadas en la nube a las instalaciones locales	12 %	1 %	26 %	9 %
SÍ (una o más razones)	88 %	99 %	74 %	91 %
SÍ, después de una recuperación ante desastres	40 %	45 %	31 %	45 %
SÍ, se migró desde las instalaciones locales y se decidió retirar de la nube	43 %	46 %	35 %	51 %
SÍ, se desarrolló en una nube y se planeó la ejecución dentro de un centro de datos	49 %	52 %	40 %	59 %

99 %

de las organizaciones devolvieron las cargas de trabajo a sus centros de datos por alguna razón, incluido el failback de recuperación ante desastres, la preparación frente a la producción o la reconciliación de que la nube no era óptima para esa carga de trabajo

Teniendo en cuenta la combinación diversa en cuanto a dónde se originan las cargas de trabajo alojadas en la nube, así como las innumerables razones por las que las cargas de trabajo vuelven a las instalaciones locales, las estrategias de protección de datos en 2023 no solo deben hacer backup de las cargas de trabajo alojadas en la nube después de que se las coloque allí, sino también, idealmente, deben ser capaces de ayudar en la migración de la nube al centro de datos o de una nube a otra nube, según los requisitos empresariales.

Bases de datos y archivos compartidos alojados en la nube

Las infraestructuras alojadas en la nube ofrecen una variedad de funcionalidades para **compartir archivos**, que incluyen:

- El **76 %** ejecuta archivos compartidos que se ejecutan dentro de instancias de servidores alojadas (p. ej., recursos compartidos de Windows Server o Cloud ONTAP)
- El **56 %** ejecuta servicios de archivos compartidos (SMB o NFS) desde el propio proveedor de nube a hiperescala

Con un impulso similar de los archivos compartidos alojados en la nube como medio principal de "datos no estructurados" que se trasladan a los servicios en la nube, los "datos estructurados" **(bases de datos)** tienen un índice de adopción similar:

- El **78 %** ejecuta bases de datos que se ejecutan dentro de instancias de servidores alojadas (p. ej., servidores de Windows o de Linux)
- El **56 %** ejecuta servicios de bases de datos gestionados desde el propio proveedor de nube a hiperescala

Ejecutar servicios básicos, como archivos compartidos y bases de datos, es un atractivo "universal" para las organizaciones de TI de todos los tamaños, pero hay algunas variaciones en el uso de estos servicios en la nube, supuestamente en función de la accesibilidad al ancho de banda y a la infraestructura de la nube.

	Internacional	América	EMEA	APJ
Archivos compartidos en instancias de servidores	76 %	**86 %**	67 %	75 %
Archivos compartidos a través de servicios gestionados	56 %	**59 %**	48 %	62 %
Bases de datos en instancias de servidores	78 %	**85 %**	71 %	76 %
Bases de datos a través de servicios gestionados	65 %	**74 %**	53 %	68 %

De hecho, el **91 %** de las organizaciones globales encuestadas ejecuta servicios de archivos o bases de datos de uno o más proveedores de nube. Por lo tanto, si bien las instancias de servidores lifted+shifted (realojadas) siguen siendo mayoría, la combinación diversa sugiere que las estrategias de protección de datos en 2023 y más allá para entornos alojados en la nube DEBEN proteger la gama de archivos compartidos y de bases de datos que ahora se ejecutan desde los servicios en la nube. Sorprendentemente, algunas organizaciones subestiman la importancia de las versiones anteriores y de la retención a largo plazo para los datos alojados en la nube, cuando los servicios de PaaS son duraderos de forma nativa. De hecho, la resiliencia de los servicios en la nube a veces puede llevar, equívocamente, a las organizaciones a no hacer backup de sus cargas de trabajo alojadas en la nube:

- El **34 %** cree que sus **archivos compartidos** alojados en la nube son duraderos o que no necesitan backup
- El **15 %** cree que sus **bases de datos** alojadas en la nube son duraderas o que no necesitan backup

Están equivocados.

91 %

de las organizaciones ejecutan archivos compartidos o bases de datos de producción desde una nube con alguna combinación de instancias de servidores y servicios gestionados.

A medida que las ofertas maduren y las organizaciones se sientan más cómodas, es probable que la combinación de instancias de servidores se reduzca gradualmente, y los servicios gestionados aumenten de manera más significativa.

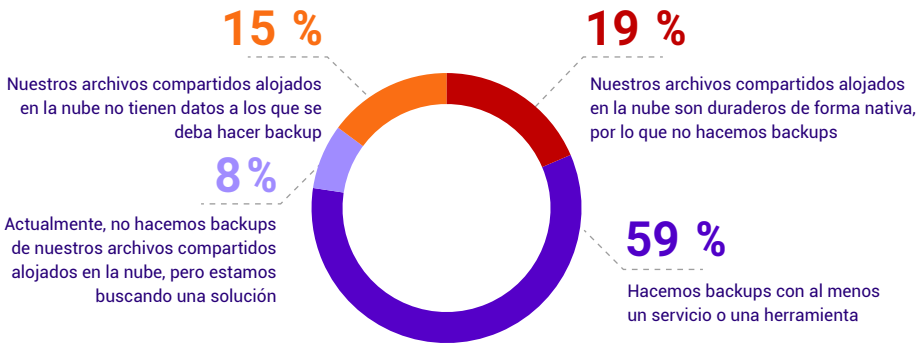


Figura 2.5

¿Cómo hace backups de los datos dentro de sus archivos compartidos en Amazon o en Azure?

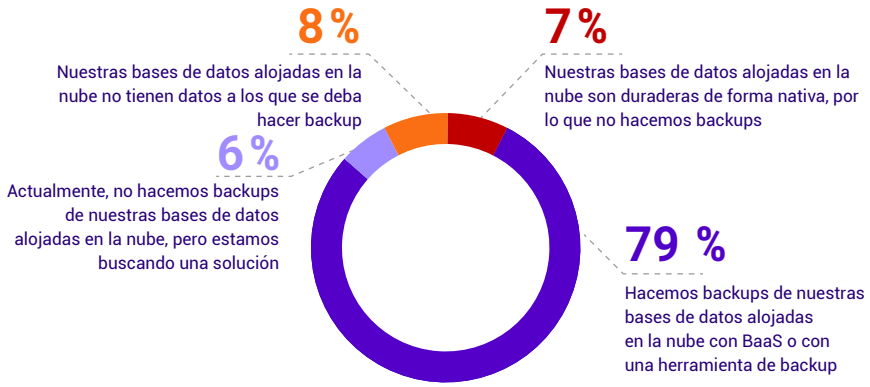


Figura 2.6

¿Cómo hace backups de sus bases de datos que se ejecutan en Amazon o en Azure?

Varios equipos afectan la estrategia de protección de datos, pero los backups son backups

Los entornos alojados en la nube de hoy en día reciben una gama aún mejor de aportes que incluyen a especialistas en la nube y a los propietarios de las aplicaciones, incluso más que el año anterior.

Una vez establecida la estrategia, la mayoría de los backups de las cargas de trabajo alojadas en la nube es realizada por el mismo equipo que hace el backup de las cargas de trabajo del centro de datos, con un margen de 2:1 = administradores de backups **(69 %)** frente a administradores de la nube **(31 %)**.

Para las organizaciones que utilizan Backup as a Service (backup como servicio, BaaS) para sus cargas de trabajo alojadas en la nube, los integrantes del equipo de BaaS administran los trabajos de backup una cuarta parte del tiempo, y los equipos de backup y de nube aún mantienen una proporción de **2:1** de los trabajos autogestionados, proporcionalmente.

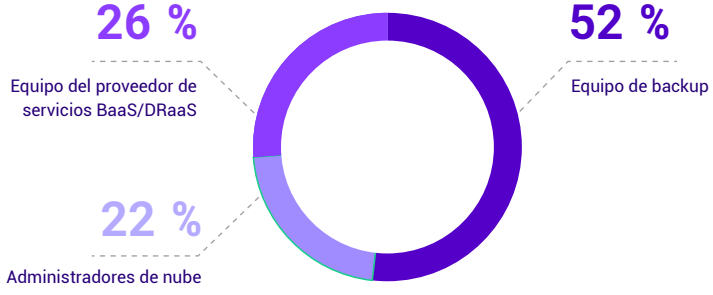


Figura 1.4

En general, ¿quién administra los backups y la protección de datos de los servidores alojados en la nube, en su organización?

Derribamos los mitos sobre el backup de los servicios de M365

Hay dos suposiciones comunes respecto de SaaS y de la protección de datos:

- La función integrada de papelera de reciclaje/deshacer/retener es lo suficientemente buena como backup
- Los administradores de aplicaciones no entienden que los backups son importantes

Ambas suposiciones son incorrectas. Al principio de la mayoría de los viajes "como servicio" de producción, muchas organizaciones asumen, incorrectamente, que la resiliencia del servidor o las funciones integradas de "deshacer" desmienten la necesidad de un backup. Esta confusión era válida en los inicios de M365; agravada por funcionalidades mejoradas como "retención legal" en las ofertas prémium. Hoy en día, solo el **4 %** confía, nada más, en la papelera de reciclaje de M365 o en funcionalidades similares para deshacer, y, afortunadamente, solo el **3 %** cree, por error, que la resiliencia de M365 desmiente la necesidad de backups. Para el otro **93 %** de las organizaciones con M365:

- La mayoría del **43 %** que utiliza los niveles mejorados de M365 entiende que esas funcionalidades están diseñadas para escenarios que no sean "backup" o retención a largo plazo
- Más de 3 de cada 4 **(78 %)** utilizan un producto de backup de terceros o BaaS con el fin de hacer backup de M365

Vale la pena señalar que el repositorio más común para datos de M365 a largo plazo es Azure Storage, utilizado por el **42 %** de las organizaciones, que puede permitir excelentes escenarios de recuperación si se utilizan diferentes credenciales con el fin de minimizar los escenarios cibernéticos.

Otro malentendido común entre los propietarios de las aplicaciones y los administradores de backup son las innumerables razones para proteger los datos. Si bien la preocupación principal de los propietarios de las aplicaciones puede ser el tiempo de actividad y solo el rollback relativamente reciente, los administradores de backup tienden a enfocarse en los mandatos de cumplimiento y en los desastres cibernéticos y de otro tipo. El siguiente cuadro es positivo, ya que tanto los administradores de M365 como los especialistas en backups coinciden, en su mayoría, en las razones más importantes para hacer un backup de los datos de M365.

No hace mucho tiempo que la papelera de reciclaje integrada era "lo suficientemente buena" para la mayoría de las organizaciones que aún no reconocían la necesidad de backups reales de M365.

En 2021, el **47 %** dependía, únicamente, de la papelera de reciclaje, en comparación con el **4 %** actual. Mientras tanto, el **78 %** ahora utiliza un backup de terceros, en comparación con el **45 %** en 2021.

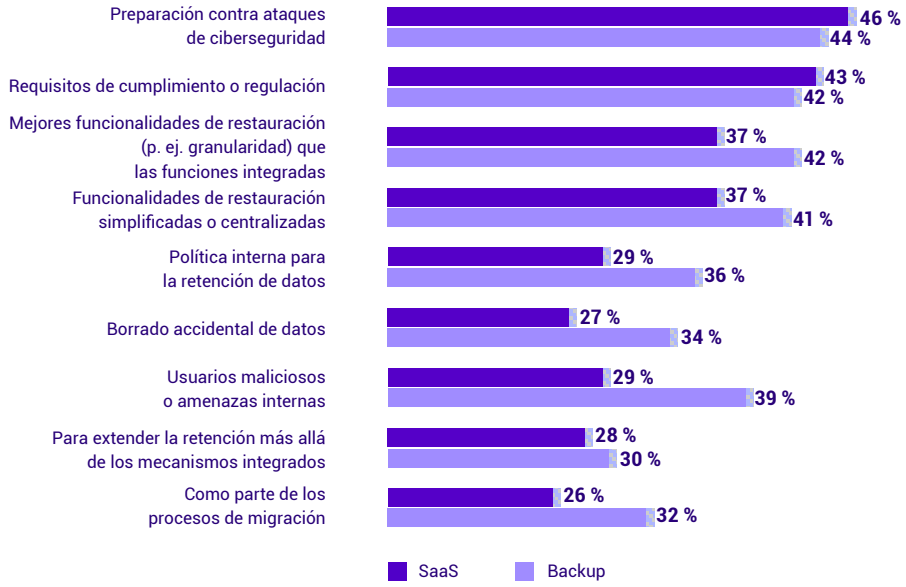


Figura 3.4

¿Cuáles son los motivos principales de su organización para hacer un backup de sus datos en Microsoft 365?

¿Por qué elegir BaaS o DRaaS?

Al considerar los servicios de protección de datos basados en la nube, es importante tener claras las diferencias:

- Backup as a Service (backup como servicio, BaaS), enfocado en proteger y restaurar datos a través de un repositorio y servicio en la nube
- Disaster Recovery as a Service (disaster recovery como servicio, DRaaS), enfocado en reanudar la funcionalidad mediante el uso de infraestructura alojada en la nube en lugar de un sitio secundario de "failover"

Empiece por hacerse la pregunta más fundamental de cualquier servicio en la nube: *"¿Cuáles son los beneficios de (BaaS o DRaaS) en comparación con administrar mi propia solución?"*

- **En el caso de BaaS,** la respuesta es la *eficiencia operativa.* Además de la capacidad de supervivencia y la agilidad de los datos (es decir, la capacidad de acceder a los backups en cualquier lugar), las cinco razones más comunes se reducen a la eficiencia operativa.
- **En el caso de DRaaS,** los encuestados reconocieron una variedad más amplia de justificaciones. Las tres justificaciones más importantes tuvieron que ver con la *experiencia* que un proveedor de DRaaS ofrece como complemento al personal de TI:
  - Experiencia en la implementación
  - Experiencia en la planeación
  - Mayor disponibilidad de los expertos internos del personal de TI para realizar otras tareas

Solo después de las justificaciones de la experiencia, vemos eficiencias, funcionalidades mejoradas y monitorización, es decir, las justificaciones para BaaS. Dicho de otra manera, si bien puede considerarse que BaaS ofrece mejoras tácticas, DRaaS se justifica por sus beneficios estratégicos para la organización.

81 %

de las organizaciones prevé utilizar protección de datos basada en la nube (BaaS o DRaaS) antes de 2023.

http://vee.am/DPR22

El camino hacia la protección basada en la nube

Hoy en día, el **42 %** utiliza el almacenamiento en la nube dentro de su solución de backup del centro de datos, mientras que el **58 %** utiliza BaaS, pero eso no es lo más interesante.

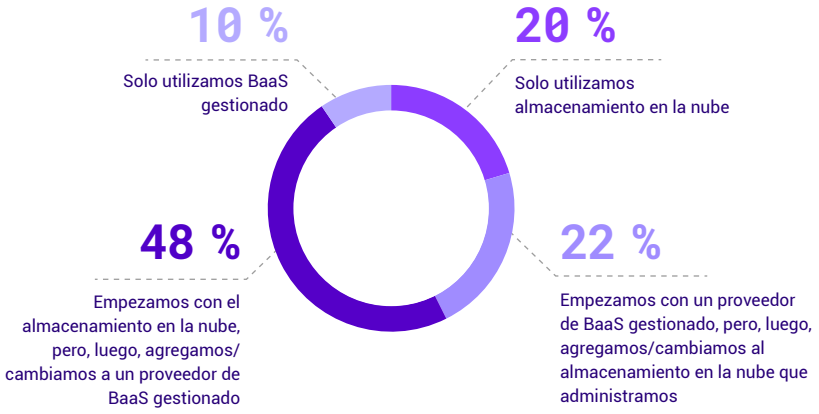


Figura 5.1

¿Cómo describiría el uso y la experiencia de su organización con los servicios/el almacenamiento de backups en la nube?

Una de las nuevas preguntas más potentes dentro del informe sobre tendencias de protección en la nube de este año fue cuando se preguntó a los encuestados cómo agregaron, por primera vez, las funcionalidades de la nube a su estrategia de protección de datos:

- Primero utilizaron almacenamiento en la nube, como parte de una solución de protección de datos tradicional
- Primero se inscribieron en una suscripción a BaaS gestionada

¿Cuál es su situación actual?

- El **30 %** no cambió respecto del inicio
- El **70 %** cambió de autogestionado a BaaS o viceversa

De los que cambiaron, casi 2:1 cambiaron A BaaS DESDE el almacenamiento en la nube (en lugar de desde BaaS al almacenamiento en la nube), lo que significa que muchos empezaron con backups autogestionados que utilizaban almacenamiento en la nube (p. ej., bucket/blob a hiperescala), pero pasaron a adoptar el resto de lo que ofrecen los proveedores de servicios: experiencia. Mientras que el **22 %** empezó con BaaS, pero, luego, decidió ejecutar sus propios repositorios en la nube, casi la mitad de los encuestados **(48 %)** empezó con almacenamiento en la nube sencillo y, luego, optó por utilizar BaaS en su lugar.

Vale la pena señalar que estas estadísticas varían según la región:

	Internacional	América	EMEA	APJ
Uso exclusivo de almacenamiento en la nube	20 %	**26 %**	15 %	19 %
Inicialmente, BaaS gestionado; pero, luego, almacenamiento en la nube	22 %	**38 %**	58 %	47 %
Inicialmente, almacenamiento en la nube; pero, luego, BaaS gestionado	48 %	**21 %**	20 %	27 %
Uso exclusivo de BaaS gestionado	10 %	**14 %**	7 %	7 %

Podría decirse que no hay ninguna respuesta incorrecta con respecto a qué tipo de nube o quién la administra:

- Casi la mitad **(46 %)** de las organizaciones opta por autogestionar sus trabajos de backup, pero confía en un proveedor de BaaS para mantener el servidor o los servicios de backup; esto por sí solo puede aliviar, significativamente, a los equipos de TI al eliminar la atención continua y la gestión de servidores de backup, almacenamiento, parches de software, etc.
- Un tercio **(31 %)** de las organizaciones prefiere delegar la mayoría de las operaciones de backup (p. ej., monitorización de trabajos de backup, capacity planning (planeación de la capacidad), alertas e incluso tareas de restauración) a los centros de asistencia de BaaS.

Y, como de costumbre, hay algunas variaciones por región:

	Internacional	América	EMEA	APJ
Mayormente, gestión de TI	46 %	**45 %**	50 %	41 %
Equilibrio de TI y MSP	23 %	**18 %**	24 %	28 %
Mayormente, gestión de MSP	31 %	**36 %**	26 %	31 %

Los cambios del almacenamiento en la nube a BaaS gestionado pueden verse mejor cuando se observa el mayor interés en los servicios BaaS preconfigurados o "de guante blanco".

En 2021, solo el **13 %** quería que su proveedor de servicios se encargara de la mayor parte de la gestión, pero, ahora, el porcentaje es **31 %**. Mientras tanto, el **46 %** actualmente quiere administrar sus propios servicios. Dicha cifra es inferior al **63 %** en 2021.

La perspectiva de Veeam

Plataforma de backup y gestión de datos de Veeam

Ahora más que nunca, es crítico para los negocios permanecer confiados en que sus datos están protegidos y siempre disponibles, ya sea en las instalaciones locales, en los extremos o en la nube. Veeam brinda una plataforma única para entornos en la nube, virtuales, físicos, de SaaS y de Kubernetes. Nuestros clientes están seguros de que sus aplicaciones y datos están protegidos contra el ransomware, los desastres y los actores maliciosos, y que están siempre disponibles con la plataforma más sencilla, flexible, confiable y potente de la industria.

Veeam les da a los clientes la confianza para acelerar la transformación digital, protegerse contra el ciberdelito e impulsar la resiliencia del negocio, lo que garantiza que sus datos estén siempre protegidos y disponibles. Reduzca los costos y la complejidad, y logre sus objetivos comerciales con Veeam: el backup y recuperación n.º 1.

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

Haga clic aquí para ver el informe de investigación global completo

Si tiene preguntas relacionadas con la información de la investigación, puede escribir a StrategicResearch@veeam.com