veeam

# 8 Beneficios de un servicio de backup para IaaS, PaaS y SaaS

# Los 8 beneficios


1. Ahorro de tiempo y dinero 4

2. Protección de datos sencilla y recuperación confiable 5

3. Configuración rápida y sin complicaciones 6

4. Servicio escalable, de alta velocidad y con todo incluido 7

5. Almacenamiento y retención escalables 8

6. Seguridad, inmutabilidad y arquitectura resiliente 9

7. Integridad de datos confiable y preparada para el cumplimiento 10

8. Diseñado a medida para sus cargas de trabajo con recuperación contextual 11


© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# Introducción

Sus datos empresariales más críticos ahora residen en plataformas SaaS y en la nube que no controla. Microsoft 365 es donde su equipo colabora, Entra ID decide quién puede acceder, Salesforce almacena su proceso de ventas e historial de ingresos, y Azure y AWS gestionan la infraestructura subyacente que sustenta todo. Estas plataformas son productivas, rápidas y están profundamente conectadas entre sí. Esa conectividad es también lo que las hace vulnerables.

La identidad es ahora la principal superficie de ataque. Microsoft registra miles de ataques basados en credenciales por segundo. Una vez que un atacante se mueve por su entorno con credenciales de confianza, puede modificar, eliminar o exfiltrar datos de forma silenciosa en todos los sistemas conectados. En el momento en que se descubre la violación, la retención nativa ya ha preservado el estado comprometido, no la versión limpia que su empresa necesita restaurar.

El modelo de responsabilidad compartida lo hace explícito: los proveedores de SaaS protegen la plataforma; usted protege los datos. Eso convierte a la estrategia de backup en una de las decisiones más trascendentales que debe tomar su equipo de TI. Y con la creciente presión de hacer más con equipos más reducidos, encontrar el tiempo, el dinero y el talento para mantener una protección confiable, basada en la identidad, en múltiples entornos puede parecer imposible.

El backup solo por software para una sola carga de trabajo fue diseñado para entornos predecibles y restauraciones a nivel de elementos. Falla cuando se necesita resiliencia en colaboración, identidad, CRM e infraestructura en la nube, especialmente cuando es necesario reconstruir miles de objetos después de un incidente de seguridad. Estas herramientas requieren mantenimiento constante, ajustes y planificación de la infraestructura, y aún tienen dificultades para lograr una recuperación íntegra a gran escala. El manejo de distintas soluciones puntuales para cada plataforma genera una proliferación de herramientas, fragmenta la visibilidad e introduce brechas que los atacantes y los auditores de cumplimiento descubrirán antes que usted.

Un servicio de backup basado en SaaS cambia el modelo. El proveedor gestiona la pila completa: infraestructura, endurecimiento de seguridad, almacenamiento, actualizaciones. Su equipo conecta los entornos y comienza a proteger los datos. Los puntos de restauración son independientes de su tenant de producción, por lo que las identidades comprometidas no pueden acceder a ellos. La recuperación funciona igual tanto si está restaurando un solo ítem como si está reconstruyendo grandes porciones de su entorno después de un incidente. Cuando ese servicio unifica la protección en su SaaS, identidad e infraestructura de nube, obtiene una vista única de su cobertura de protección, costos previsibles y la capacidad de expandirse sin agregar personal ni herramientas.

**A continuación se presentan ocho ventajas específicas de ese modelo y por qué son importantes cuando la amenaza que su backup realmente debe resistir es el compromiso de identidad.**

© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# 1. Ahorro de tiempo y dinero

Los entornos de backup tradicionales y autogestionados hacen que los costes sean casi imposibles de predecir. El mantenimiento del hardware, la optimización del almacenamiento, la aplicación de parches a las vulnerabilidades, el endurecimiento de los sistemas y la preparación para la recuperación en el peor de los casos requieren conocimientos especializados y una cantidad significativa de tiempo. La infraestructura debe sobredimensionarse por si acaso, por lo que las organizaciones rutinariamente pagan por capacidad que nunca utilizan, y aun así se enfrentan a gastos inesperados cuando el crecimiento supera la planificación. Si multiplicas eso por cada plataforma SaaS y de nube de la que depende tu negocio, el desperdicio se acumula rápidamente.

Como el proveedor administra la infraestructura, el almacenamiento, la seguridad y las actualizaciones, su equipo no tiene que hacerlo. Cualquier miembro del equipo de TI puede configurar la protección y restaurar datos con confianza, sin capacitación especializada ni temor a errores de configuración. Cuando todas las cargas de trabajo críticas residen en una sola plataforma, se elimina la proliferación de herramientas que agota silenciosamente el presupuesto y la atención. Menos ciclos de adquisición, relaciones con proveedores que gestionar y brechas entre herramientas donde el riesgo pasa desapercibido.

Los precios predecibles basados en suscripciones reemplazan los gastos de capital impredecibles y los despliegues de emergencia. Algunos proveedores de backup SaaS incluyen almacenamiento ilimitado o elástico, por lo que el crecimiento de datos no infla sus costes de forma silenciosa. La protección se escala automáticamente con su SaaS y huella en la nube. Paga por lo que usa.

El efecto neto es una estrategia de resiliencia más fácil de gestionar, más sencilla de presupuestar y que no requiere que su equipo se convierta en especialistas en infraestructura para que funcione.

El backup debe ser un elemento formal en la planificación, no una tarea secundaria.

## Backup SaaS predecible sin sobrecarga de infraestructura.

**Elimina el sobreaprovisionamiento y los costos inesperados derivados de capacity planning (planificación de la capacidad).**

**Simplifica las operaciones sin necesidad de conocimientos especializados en infraestructura.**

**Los precios de suscripción reemplazan los gastos impredecibles de capital y emergencia.**

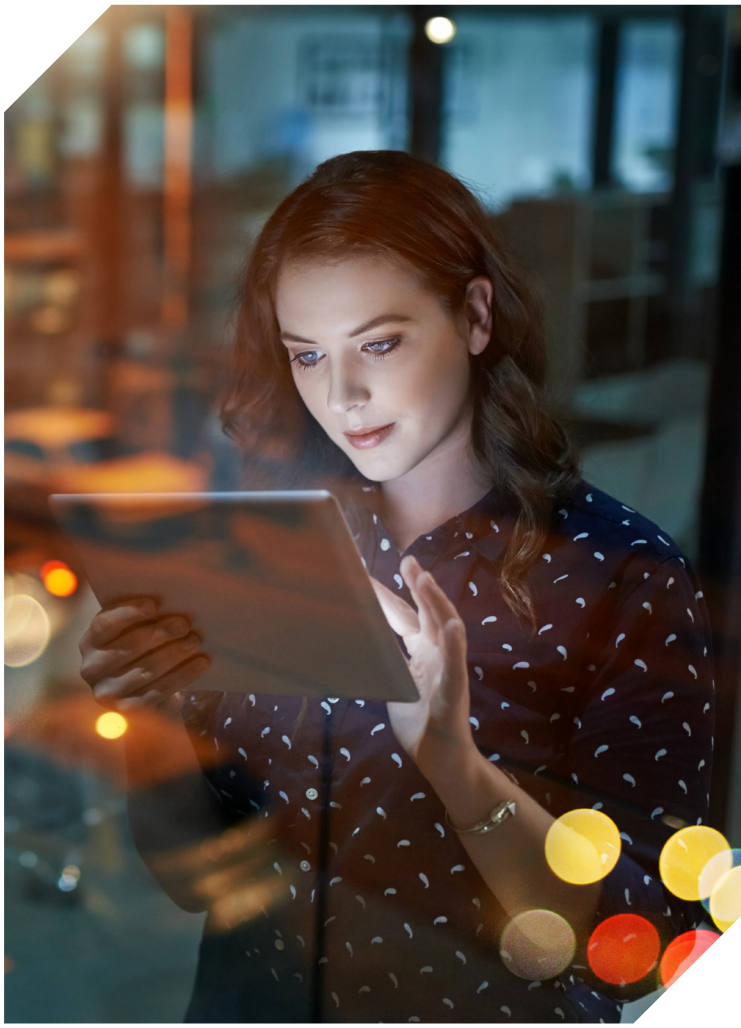
© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# 2. Protección de datos sencilla y recuperación confiable

El backup autogestionado nunca está completo. Las plataformas SaaS y en la nube cambian constantemente, y los sistemas de backup deben mantenerse al ritmo: aplicar parches, ajustar el rendimiento, escalar el almacenamiento, reforzar la seguridad. Estas son tareas perpetuas y compiten por el mismo equipo y presupuesto que el resto de responsabilidades de TI.

Un servicio de backup SaaS almacena y opera sus puntos de restauración completamente fuera de sus entornos de producción. Las identidades comprometidas, las configuraciones erróneas o los cambios maliciosos dentro de tu tenant no pueden alcanzarlos. Esa separación es el argumento central de esta sección, y vale la pena ser precisos sobre el motivo: cuando un atacante realiza cambios usando credenciales válidas, el entorno de producción deja de ser una fuente confiable de verdad. Sus backups deben serlo.

El servicio gestiona el escalado del almacenamiento, la optimización del rendimiento, la gestión de vulnerabilidades y las actualizaciones de seguridad continuas. Lo que ve su equipo es una única interfaz para configurar la protección, establecer la retención y ejecutar restauraciones. La experiencia es la misma tanto si está recuperando un correo electrónico eliminado como si está reconstruyendo configuraciones y permisos en todas las plataformas después de un incidente importante.



## Fácil de adoptar. Fácil de operar, confiable cuando la recuperación es fundamental.

© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# 3. Configuración rápida y sin complicaciones

La implementación del software de backup suele ser la peor parte. Poner en marcha los servidores, configurar el almacenamiento, cablear las redes, coordinar con los especialistas, licenciar el software correctamente y esperar que todo funcione realmente cuando se ejecute el primer backup. Cada paso conlleva un riesgo, y todos deben funcionar correctamente al mismo tiempo.

Estos sistemas tienen una curva de aprendizaje y necesitan ser re-arquitecturados cada vez que el entorno se modifica. A pesar de esa inversión, el backup tradicional sigue fallando con demasiada frecuencia. Según el Informe de tendencias de ransomware 2025 de Veeam, el 53% de las organizaciones no logra recuperarse lo suficientemente rápido como para alcanzar la productividad plena tras un incidente. Esto se debe cada vez más a que sus backups no estaban aislados del incidente basado en la identidad que causó el daño en primer lugar.

Un servicio de backup basado en SaaS elimina todo eso. No hay servidores que poner en marcha, almacenamiento que aprovisionar, ni planes de capacidad que modelar. Conecte el servicio a sus entornos SaaS, de identidad y de nube, y comience a proteger los datos en cuestión de minutos. Una plataforma que cubre todas las cargas de trabajo, con una sola implementación.

**Configure una vez, luego siga avanzando.**

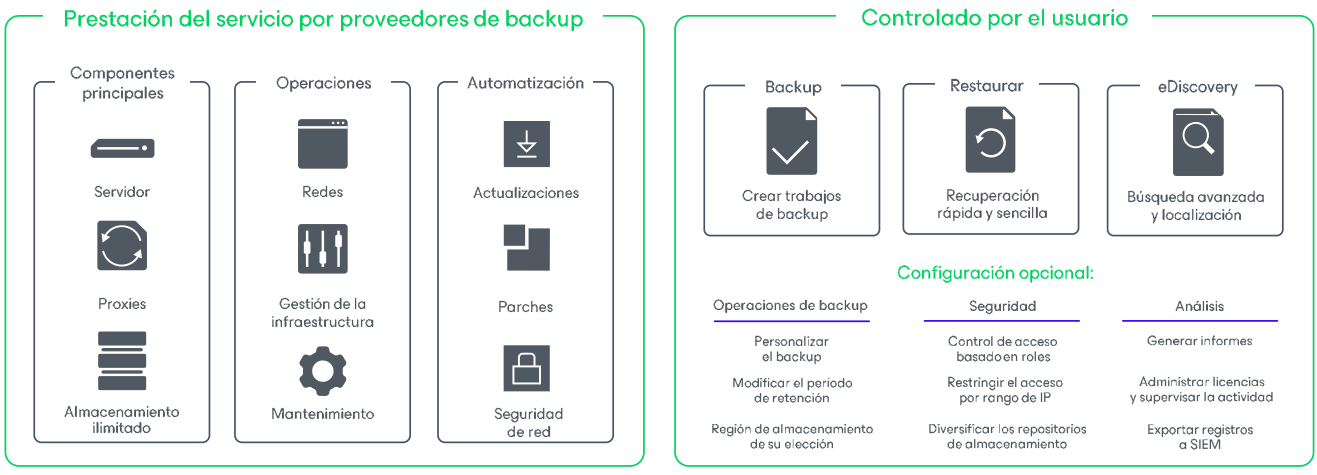
© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# 4. Servicio escalable, de alta velocidad y con todo incluido

uando las organizaciones gestionan por sí mismas sus backups, deben integrar manualmente servidores, almacenamiento y software. También asumen una amplia lista de tareas de administración continuas para mantener esos sistemas funcionando de forma eficiente. Incluso con personalización, los entornos de backup autogestionados introducen pequeños errores de configuración, puntos ciegos y deficiencias de mantenimiento que se acumulan silenciosamente y debilitan la recuperación cuando se pone a prueba.

Lo que cambia con un servicio gestionado es la velocidad de recuperación. Las plataformas de backup SaaS utilizan APIs optimizadas para backup, diseñadas para cada carga de trabajo, lo que significa que las restauraciones se realizan a velocidades que no son posibles cuando está limitado por su propio hardware y red. Eso cobra mayor importancia a escala. Cuando un incidente relacionado con la identidad afecta simultáneamente a decenas de miles de objetos en tus entornos SaaS, de identidad y de nube, las herramientas tradicionales fallan. Se diseñaron para la recuperación a nivel del elemento. La reconstrucción de cargas de trabajo múltiples es un problema completamente diferente. Los servicios de backup SaaS paralelizan estas operaciones a través de la infraestructura del proveedor, por lo que las restauraciones a gran escala no requieren que usted aprovisione hardware ni el diseño anticipado de flujos de trabajo de recuperación ante desastres.

**En este escenario, la recuperación a gran escala deja de ser un ejercicio de planificación y se convierte en una funcionalidad confiable.**




© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# 5. Almacenamiento y retención escalables

La colaboración moderna y las operaciones en la nube producen volúmenes masivos de datos: archivos, chats, versiones, registros, cuentas de usuario, membresías de grupos. La recuperación de cualquiera de ellos después de un incidente depende de la cantidad de historial que haya conservado y de si ese historial se almacena fuera del entorno que se vio comprometido.

Un servicio de backup proporcionado mediante SaaS elimina esa restricción. La plataforma escala el almacenamiento de forma elástica a medida que tus datos crecen en cada carga de trabajo protegida. Ya sea que esté restaurando un solo archivo o reconstruyendo meses de colaboración, identidad y datos críticos para el negocio después de un compromiso basado en la identidad, la capacidad de almacenamiento nunca se convierte en el cuello de botella. Muchos paquetes incluyen almacenamiento ilimitado o elástico, lo que elimina la presión del crecimiento de los datos sobre los costos de resiliencia.

La capacidad de almacenamiento es solo la mitad de la ecuación. Las plataformas SaaS conservan los datos tal y como existen actualmente, incluyendo cualquier cambio que realice un atacante usando credenciales válidas. La recuperación limpia requiere acceso a versiones anteriores intactas que reflejen cómo eran sus entornos antes de la brecha de seguridad. Con una retención flexible y a largo plazo, las organizaciones pueden mantener exactamente la profundidad histórica que necesitan para cumplimiento, descubrimiento, gobierno interno o rollback a gran escala.

El lugar donde se alojan esos datos también es importante. Las regulaciones globales dictan cuánto tiempo se conservan los datos, dónde residen y quién puede acceder a ellos. Un servicio de backup SaaS con controles de residencia integrados le permite alinear el almacenamiento con los requisitos regionales sin tener que construir una infraestructura independiente en cada región.

El resultado es una versión completa en un punto en el tiempo de su entorno a la que puede volver, sin importar cuántos datos genere, cuántas cargas de trabajo proteja o lo lejos que necesite retroceder.

## Un backup de SaaS elástico para una resiliencia de datos escalable y conforme a las normativas

**El almacenamiento elástico elimina los límites de capacidad durante las operaciones de recuperación.**

**La retención a largo plazo garantiza la disponibilidad de datos limpios anteriores a cualquier incidente de compromiso.**

**Dos controles de residencia de datos respaldan el cumplimiento de las regulaciones globales**

© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# 6. Seguridad, inmutabilidad y arquitectura resiliente

Ninguno de los beneficios anteriores importa si el backup en sí no es seguro. Con más de la mitad de las organizaciones que informan de pérdida de datos o corrupción de datos en aplicaciones SaaS durante el último año, la simplicidad operativa solo importa si su entorno de backup es tan seguro, inmutable y confiable como el que usted mismo construiría.

Los datos se cifran de extremo a extremo, en tránsito y en el destino, y se almacenan de forma inmutable. El entorno de backup opera bajo su propio dominio de autenticación, totalmente aislado de sus identidades de producción. Un atacante que comprometa las credenciales en su tenant de SaaS no podrá usar esas credenciales para acceder, modificar o eliminar copias de backup. El air-gap (entorno aislado) es un límite arquitectónico entre su entorno de producción y sus datos de recuperación.

El proveedor se encarga de la aplicación de parches, la gestión de vulnerabilidades y la monitorización en toda la pila, lo que significa que su superficie de ataque operativa se reduce continuamente sin la intervención de su equipo. La arquitectura sigue los principios de confianza cero: asumir brecha, limitar el radio de explosión y mantener una ruta de recuperación que el entorno comprometido no puede tocar. La detección de amenazas impulsada por IA identifica patrones sospechosos en las cargas de trabajo protegidas (eliminaciones masivas, cambios inusuales de permisos, modificaciones anómalas de datos) antes de que esos cambios puedan propagarse a los datos de backup.

Disponibilidad y durabilidad están integradas en la misma arquitectura. Los datos de backup se almacenan en múltiples copias redundantes en centros de datos distribuidos geográficamente y tolerantes a fallos. Si una región deja de funcionar, tus datos de recuperación siguen disponibles. El modelo de seguridad se aplica a nivel de arquitectura: inmutabilidad, aislamiento, cifrado y redundancia. Los valores predeterminados son seguros.

**Y no depende de que tu equipo acierte en todo, en todo momento.**

© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# 7. Integridad de datos confiable y preparada para el cumplimiento

El cumplimiento se vuelve más difícil cuando no puede confiar en sus propios datos. Si los datos de SaaS han sido alterados, eliminados o corrompidos por identidades comprometidas, demostrar lo que existía antes del incidente se convierte en el desafío central. Las normas reglamentarias dan por supuesto que usted puede generar registros limpios e históricos bajo demanda. Sin un backup independiente, puede que no sea posible hacerlo.

Las herramientas nativas de gobierno preservan los datos en su estado actual. No preservan estados históricos. Si la información fue modificada, incluso por una identidad legítima, puede que no quede ninguna versión limpia en el entorno de producción para entregar. Y debido a que los cambios de identidad se mezclan a la perfección en los registros de auditoría de las plataformas SaaS y nube, las organizaciones suelen tener dificultades para demostrar qué ocurrió, cuándo o por qué.

Copias independientes de un punto en el tiempo almacenadas fuera del entorno de producción sirven como evidencia que el propio entorno de producción no puede proporcionar. Durante auditorías, eDiscovery, investigaciones y revisiones regulatorias, estas versiones inmutables se convierten en el registro autoritativo: qué existió, cuándo y en qué estado.

Normativas como RGPD, DORA, HIPAA y APPI exigen requisitos estrictos sobre dónde se almacenan los datos y quién tiene acceso a ellos. Un servicio de backup de SaaS con controles de residencia integrados permite a las organizaciones determinar exactamente dónde se almacenan los datos de backup, ajustándose a los mandatos regionales sin necesidad de crear una infraestructura personalizada en cada región.

Presentar evidencia de cumplimiento en cualquier momento es tan importante como lograrlo. Los informes y registros de auditoría integrados proporcionan un rastro claro y exportable de la actividad de backup, el estado de retención y el historial de restauración. Cuando los auditores o los equipos legales solicitan pruebas de que los datos fueron protegidos, retenidos y recuperables, dicha evidencia ya existe.

Los proveedores de servicios de backup SaaS se someten regularmente a auditorías de terceros (SOC 2 Tipo II, ISO 27001 y otras, según el proveedor) para validar que sus prácticas de seguridad y gestión de datos resisten el escrutinio externo. Esas certificaciones pasan a formar parte de su postura de cumplimiento por extensión.

**El cumplimiento nunca debería ser una sorpresa, y no tiene por qué serlo.**

© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# 8. Diseñado a medida para sus cargas de trabajo con recuperación contextual

Los datos críticos no residen en un solo lugar:

- Microsoft 365 impulsa la colaboración
- Entra ID rige el acceso
- Salesforce almacena inteligencia del cliente, pipeline y registros de operaciones
- Azure y AWS alojan la infraestructura que integra todos los componentes

Cada plataforma tiene su propia arquitectura, API y reglas sobre el modo en que interactúan los datos, los permisos y las políticas. Si un backup trata estos elementos como intercambiables, generará recuperaciones que serán como mínimo incompletas y como máximo engañosas. El backup diseñado especialmente resuelve esto diseñando la protección en torno al modelo de objetos y las API específicas de cada plataforma.

Para Microsoft 365 y Entra ID, eso significa emplear API optimizadas para backups, que proporcionan backups y restauraciones mucho más rápidos que el software ejecutado en el hardware del cliente. Y lo que es más importante, el backup captura el contexto entre los objetos: datos de Exchange, sitios de SharePoint, contenido de OneDrive, permisos de Entra ID, membresías de grupos y registros de aplicaciones. La restauración devuelve el entorno tal y como existía. Cuando los incidentes impulsados por la identidad afectan a miles de objetos a la vez, esa es la diferencia entre un rollback limpio y semanas de reconciliación manual.

La protección de Salesforce se basa en el modelo de datos único de la plataforma, que conserva registros, metadatos, archivos adjuntos y sus relaciones. Restaurar un registro de cuenta sin sus contactos, oportunidades u objetos personalizados asociados crea más confusión de la que resuelve. El backup diseñado especialmente captura estas dependencias para que los administradores puedan restaurar con total confianza.

La protección de Azure abarca máquinas virtuales, discos administrados, cuentas de almacenamiento y la capa de infraestructura que soporta operaciones híbridas y nativas de la nube. Una VM depende de su disco administrado, su configuración de red y su pertenencia al grupo de recursos. El backup que captura esas dependencias produce puntos de restauración que reflejan el estado actual de producción. Backup que no produce puntos de restauración que parecen completos hasta que se intenta arrancarlos.

En las cuatro cargas de trabajo, el principio es el mismo: los permisos, las políticas, las membresías de grupos y las dependencias entre plataformas se restauran al mismo tiempo que los datos, de modo que el entorno vuelve a ser operativo. Cuando falta ese contexto, las restauraciones pueden completarse en papel mientras el acceso se rompe, los flujos de trabajo fallan y las fronteras de confianza se desplazan de maneras que son difíciles de deshacer.

**La protección diseñada específicamente significa que se utilizan los API de cada plataforma de manera precisa, la recuperación a nivel del elemento permite reparaciones precisas, y la reconstrucción a gran escala es posible cuando los incidentes se extienden a través de sistemas conectados.**

© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

# Resiliencia de datos SaaS con Veeam Data Cloud

Cuando el backup se entrega como un servicio para SaaS y carga de trabajo en la nube, los fundamentos cambian: menor tiempo para la protección, operaciones más simples, almacenamiento y retención que se escalan con tu entorno, y una recuperación que resiste tanto incidentes relacionados con la identidad como errores cotidianos.

A través de sus entornos SaaS, de nube y de identidad, todo se reduce a esto: puntos de restauración independientes en los que puede confiar y una recuperación lo suficientemente rápida como para reconstruir lo que importa antes de que el impacto en el negocio se agrave. Veeam Data Cloud ofrece esto a través de tres funcionalidades:

- **Resiliencia alcanzada.** Automatización de políticas, protección basada en políticas y recuperaciones precisas y rápidas para que las operaciones sigan funcionando con una mínima interrupción. La información práctica obtenida mediante la monitorización, informes y análisis ayuda a validar la protección y resolver problemas.
- **Seguridad integrada.** Protección ciberresiliente integrada mediante air-gap (entorno aislado), inmutabilidad, cifrado y más. La inteligencia de amenazas ayuda a detectar y responder ante el ransomware y las amenazas relacionadas. El Control de acceso basado en roles (RBAC) común centraliza y estandariza los permisos de acceso según aplicación y rol.
- **Excelencia operativa.** La paquetización predecible y todo incluido, junto con una interfaz de usuario/UX unificada para múltiples cargas de trabajo, reducen la sobrecarga de la infraestructura y mejoran la usabilidad. La eficiencia a escala facilita superar las brechas de experiencia y disminuir el esfuerzo operativo. La aceleración de IA ayuda a optimizar las necesidades de backup, seguridad y recuperación, liberando tiempo y recursos.

Veeam Data Cloud se posiciona como la plataforma unificada en la nube para la resiliencia de datos, que ofrece tecnología de resiliencia de datos líder en la industria con la simplicidad de un servicio. Proporciona protección de datos resiliente y recuperación de datos para datos multicloud mediante servicios de backup nativo de la nube y almacenamiento, empaquetados como una oferta SaaS que incluye software de backup, infraestructura y almacenamiento en una sola solución.

**Veeam es la empresa de confianza en datos e inteligencia artificial.**

Veeam es la empresa de confianza en datos e inteligencia artificial, especializada en ayudar a las organizaciones a garantizar que sus datos y su IA sean plenamente comprendidos, protegidos y resilientes para permitir la aceleración de la IA segura a escala. Como líder del mercado tanto en resiliencia de datos como en gestión de la postura de seguridad de datos, Veeam está diseñado para la convergencia de la identidad, los datos, la seguridad y los riesgos de IA.

Veeam proporciona una inteligencia contextual profunda en cada activo de datos, identidad y modelo de IA. La empresa gobierna el acceso tanto de humanos como de agentes de IA, automatiza los procesos de privacidad, cumplimiento y remediación, y protege y recupera a las organizaciones frente a amenazas modernas —incluyendo ransomware, desastres, errores de IA, y garantizando la restauración de datos limpios y confiables. Veeam permite a las organizaciones ir más allá de la simple protección de datos, permitiéndoles aprovechar y liberar todo su potencial.

Con sede en Seattle y oficinas en más de 30 países, Veeam protege a más de 550 000 clientes en todo el mundo, incluyendo al 82% de las empresas Fortune 500, que confían en Veeam para mantener sus negocios en funcionamiento. Más información en www.veeam.com o siga a Veeam en LinkedIn @veeam-software y X @veeam.

Más información en www.veeam.com o siga a Veeam en LinkedIn @veeam-software y X@veeam.

**Más información en veeam.com**

© 2026 Veeam Software. Información confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.