Sus primeros 100 días con Veeam Data Platform

Guía para líderes sobre la resiliencia medible

La mayoría de las organizaciones asumen que están protegidas, pero pocas lo han comprobado.

En una encuesta reciente, el 90% de los líderes de seguridad afirmaron que podrían recuperar sus datos dentro de sus objetivos de recuperación definidos. Sin embargo, entre las víctimas de ransomware, solo el 28% recuperó íntegramente sus datos (Fuente: Informe sobre Confianza y Resiliencia de los Datos 2026). La confianza no es lo mismo que la funcionalidad de recuperación demostrada, y la brecha entre ambas es donde el ransomware gana, las auditorías fracasan y las interrupciones se convierten en crisis.

90%

de los líderes de seguridad afirmaron que pudieron recuperar sus datos dentro de sus objetivos definidos.

28%

de las víctimas de ransomware recuperaron sus datos en su totalidad

Porque la resiliencia solo es real cuando se puede demostrar.

Esta guía adopta una perspectiva estratégica de la implementación de Veeam Data Platform. Conforme su equipo completa los hitos técnicos de implementación, esta Guía los traduce en resultados empresariales: los riesgos mitigados, las funcionalidades desarrolladas y la evidencia que tendrá al finalizar.

Porque las decisiones sobre la tolerancia al riesgo, los compromisos de recuperación y la continuidad de negocio le corresponden a usted. Esta guía detalla sus responsabilidades y lo que podrá comunicar con confianza a la junta, los auditores y las aseguradoras al llegar al día 100.

Esto es lo que esta guía pone a su disposición:

1. Los cinco resultados que separan la resiliencia probada de la protección supuesta
2. Qué implica para su rol: CIO, CISO o CFO
3. Los siete casos de uso que cubre su inversión y cómo su implementación impulsa el ROI
4. Las preguntas que debe hacer a su equipo para confirmar que la resiliencia persiste después del día 100.

De la exposición a la evidencia: los cinco resultados que importan

Estos son los cinco resultados a los que se compromete su organización cuando implementa Veeam Data Platform. Cada uno representa un paso para pasar de la exposición a la evidencia y, juntos, definen cómo es un entorno resiliente verificable.

01. Implementado

Sabe exactamente qué está protegido, dónde se aloja y según qué estándar. Sin suposiciones y sin brechas que se descubren bajo presión.

02. Protegido

Cada carga de trabajo crítica está cubierta por un plan que respalda su estrategia de continuidad de negocio. Nada se pasa por alto cuando más importa.

03. Reforzado

Un atacante no puede destruir su capacidad de recuperación. Existen copias inmutables localmente y off-site, lo que le proporciona un punto de restauración limpio confirmado, independientemente de cómo se desarrolle el incidente.

04. Recuperación verificable

Puede demostrar que la recuperación funciona, no solo afirmarlo. Está probado, documentado y listo para presentar a su junta directiva, a sus auditores y a su aseguradora.

05. Puesta en marcha

La resiliencia no depende de una persona ni de un esfuerzo heroico. Funciona sobre responsabilidad clara, informes estructurados y una cadencia definida que su equipo puede mantener.

¿Qué significa esto para su rol

CIO/CTO

Cuando la junta directiva pregunta si su organización puede recuperarse de un incidente importante, usted tiene una respuesta probada y documentada. El riesgo de interrupción ya no es cuestión de confianza; es cuestión de documentación.

CISO

Usted tiene un punto de restauración limpio confirmado antes de que un incidente se convierta en una crisis, no después. El análisis de inteligencia sobre amenazas, las copias inmutables y los resultados de las pruebas documentados le proporcionan la evidencia que requieren sus aseguradoras, auditores y equipo legal.

CFO

La elegibilidad del ciberseguro, las condiciones de renovación y las conversaciones sobre la prima mejoran cuando la capacidad de recuperación es demostrable en lugar de asumida. Las investigaciones muestran que las organizaciones con inversiones más sólidas en resiliencia de datos pagaron un rescate solo el 33% de las veces, en comparación con el 52% de las que no lo hicieron. Su inversión en Veeam está definida, es predecible y está directamente ligada a la reducción de la exposición financiera de una interrupción no planeada.

33%

del tiempo en que las organizaciones con mayores inversiones en resiliencia de datos pagaron un rescate.

52%

del tiempo en que las organizaciones sin esas inversiones pagaron un rescate.

Fuente: Informe de Confianza y Resiliencia de Datos (2026).

Valor desbloqueado

El valor que ofrece Veeam Data Platform se extiende mucho más allá de un solo rol o un solo incidente. A partir de los primeros 100 días, su organización desbloquea funcionalidades que abordan la verdadera complejidad de los entornos de TI modernos: infraestructura híbrida, proliferación de la nube, presión regulatoria y un panorama de amenazas en constante evolución.

Estos son los siete casos de uso que su inversión está diseñada para cubrir.

Proteger y recuperar

Cuando se produce un incidente, la calidad de su respuesta depende totalmente de la calidad de su preparación. Este es el punto de partida que toda organización necesita, independientemente del sector o la infraestructura.

1. **Detección y respuesta ante amenazas:** Veeam escanea las cadenas de backup en busca de indicadores de malware y verifica la integridad de los archivos antes de la restauración, para que su organización recupere una versión limpia en lugar de reintroducir una amenaza. Los resultados documentados del escaneo respaldan su proceso de respuesta a incidentes y cumplen con los requisitos de las aseguradoras.
2. **Recuperación ante desastres a la nube:** cuando falla la infraestructura en las instalaciones locales, Veeam transfiere las cargas de trabajo a destinos en la nube dentro de sus objetivos de recuperación definidos. Su equipo cuenta con un plan probado y ejecutable, en lugar de un proceso manual que no puede funcionar bien bajo presión.

Controlar y cumplir

La presión regulatoria y los requisitos de soberanía de datos se están expandiendo. Su estrategia de protección de datos necesita mantenerse al día. Si opera en un sector regulado o está por iniciar un ciclo de auditoría, aquí es donde debe enfocarse primero.

3. **Gobierno, riesgo y cumplimiento:** Veeam genera los informes listos para auditoría que necesitan sus equipos de cumplimiento y legales, incluyendo resultados de pruebas de recuperación, inventario de cobertura y confirmación de política de retención, sin recopilar evidencia manual durante la auditoría.
4. **Soberanía:** Veeam brinda a su organización control sobre dónde se almacenan y procesan los datos de backup, respaldando los requisitos de residencia de datos a través de las jurisdicciones sin sacrificar la capacidad de recuperación.

Operar a través de la complejidad

La infraestructura moderna no se encuentra en un solo lugar. Su estrategia de protección tampoco debería estarlo. Si está en proceso de migración o ya opera en entornos multicloud o SaaS híbrido, aquí es donde se concentra el riesgo operativo.

5. **Movilidad de cargas de trabajo entre entornos:** a medida que las cargas de trabajo se trasladan entre instalaciones locales, nube y edge, Veeam traslada la protección junto con ellas. La cobertura no se rompe cuando cambia su infraestructura.
6. **Protección multicloud:** Veeam proporciona funcionalidades consistentes de protección y recuperación en los proveedores de nube, eliminando el riesgo operativo de herramientas fragmentadas y puntos ciegos entre plataformas.
7. **SaaS híbrido:** los datos críticos contenidos en las aplicaciones SaaS se protegen junto con las cargas de trabajo de su infraestructura, cerrando así la brecha de cobertura que la mayoría de las organizaciones descubren solo después de un incidente.

No se trata de funcionalidades futuras ni de complementos opcionales. Son los beneficios que obtiene su organización a medida que avanza en la implementación y activación, cada uno reduciendo una categoría específica de riesgo y fortaleciendo la confianza de su equipo directivo cuando la presión aumenta. La pregunta no es si su organización necesita este nivel de resiliencia; es qué tan rápido puede alcanzarlo.

El día 100 no es la línea de meta. Es la línea de base. La resiliencia es una práctica, no un proyecto.

Veeam proporciona la Veeam DataAI Command Platform, el modelo probado de madurez de confianza de datos e IA y los conocimientos técnicos necesarios para guiar a su equipo desde la primera implementación hasta una resiliencia plenamente demostrada. Estamos para ayudarles en cada paso del camino.

Asegúrese de que su equipo tenga la Guía técnica de los primeros 100 días y comience a alinear el alcance, el cronograma y los resultados de la implementación.

La resiliencia a este nivel no es una ambición a largo plazo. Con el plan de implementación adecuado, será una realidad a corto plazo para su organización.

El siguiente movimiento es suyo.

Preguntas que vale la pena hacer periódicamente a su equipo

- ¿Están cubiertas todas las cargas de trabajo críticas, y quedan brechas o fallas de protección sin abordar?
- ¿Cuándo realizamos la última prueba de recuperación total en condiciones reales, y disponemos de resultados documentados que lo acrediten?
- Si el ransomware atacara esta noche, ¿podríamos identificar un punto de restauración limpio confirmado y recuperar nuestros sistemas sin pagar un rescate?
- ¿Pueden nuestros equipos de cumplimiento y legales generar evidencia de auditoría sin intervención manual, y sigue nuestra arquitectura cumpliendo con nuestras obligaciones regulatorias actuales?
- ¿Quién tiene acceso administrativo a nuestro entorno de backup y cuándo fue la última vez que lo revisamos?

Acerca de Veeam Software

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. Con sede en Seattle y oficinas en más de 30 países, Veeam protege a más de 550,000 clientes a nivel mundial, incluyendo al 82% de las empresas del Fortune 500. Para más información visite www.veeam.com o síganos en LinkedIn @veeam-software y X @veeam.

Más información: veeam.com

