Veeam Data Platform

Primeros 100 días

Una guía práctica de incorporación para administradores de TI

Contenido

1. Resumen ejecutivo

Veeam Data Platform es la base para la resiliencia contra el ransomware y la continuidad operativa de su organización. Esta guía está diseñada para ayudar a los equipos de TI a implementar y desarrollar su entorno de manera estructurada. Aunque usamos el término "primeros 100 días", es solo una metáfora de una línea de tiempo. Cada organización es diferente y puede avanzar a ritmos distintos, pero el objetivo es el mismo: pasar de la configuración inicial a un estado más seguro, resiliente y listo para la recuperación. Está estructurado en torno a hitos prácticos y resultados recomendados en lugar de estrictos requisitos de implementación, lo que le permite centrarse en los pasos más relevantes para su entorno y edición.

2. ¿A quién está dirigida esta guía?

Esta guía está dirigida a **administradores de TI** que implementan, configuran y ponen en funcionamiento Veeam Data Platform. Supone que está familiarizado con la infraestructura virtual (por ejemplo, VMware vSphere, Microsoft Hyper-V o cualquier otro hipervisor compatible con Veeam Backup & Replication) y la administración básica de Windows Server. No se requieren conocimientos de Linux.

También sirve como referencia compartida para **gerentes de TI** que realizan un seguimiento del alcance y los plazos, las partes interesadas en seguridad y cumplimiento que validan la postura de endurecimiento, y los equipos de liderazgo o adquisiciones al definir cómo se ve el éxito del día 100.

3. Lo que logrará en el día 100

Para el día 100, tendrá un entorno estable, reforzado y recuperable de forma verificable que reduce el riesgo de interrupción y permite una recuperación rápida y confiable pase lo que pase.

Cada cliente debería poder confirmar que se cumplen los siguientes puntos de control:

- **Implementado:** Veeam Backup & Replication está en funcionamiento, conectado y dimensionado para satisfacer las ventanas de backup.
- **Protegido:** se hacen backups de las cargas de trabajo prioritarias según un cronograma definido.
- **Reforzado:** la inmutabilidad está implementada localmente y offsite para defenderse del ransomware.
- **Recuperable de forma verificable:** las pruebas de restauración se completan, documentan y se alinean con el objetivo de tiempo de recuperación y el objetivo de punto de recuperación (RTO y RPO).
- **Operativo:** la monitorización, las alertas, los informes y los runbooks de recuperación están implementados y bajo responsabilidad definida.

4. Hoja de ruta de un vistazo

Esta guía consta de cuatro fases secuenciales, cada una enfocada en lograr los resultados del día 100.

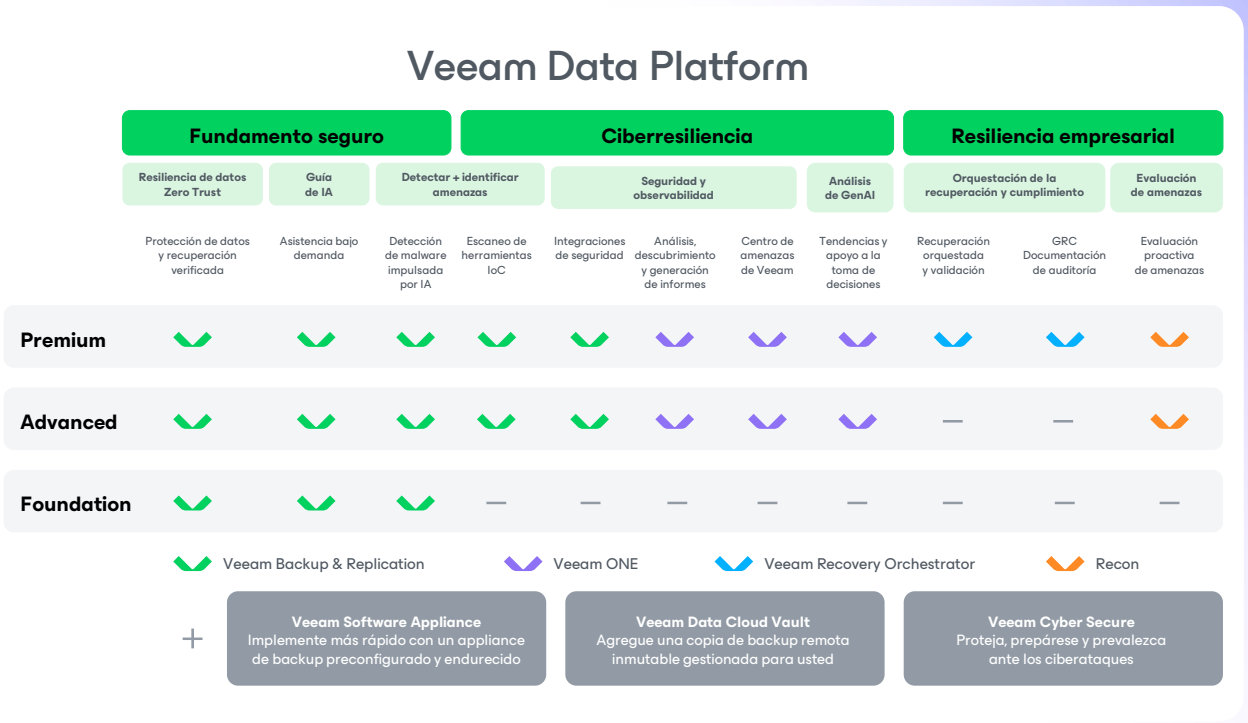
Fase	Nombre	Línea de tiempo	Enfoque
FASE 1	Base	Días 1—14	Dimensionar el entorno, desplegar Veeam Software Appliance (y Veeam Infrastructure Appliance si corresponde), ejecutar los primeros trabajos de backup, preparar para Veeam Recovery Orchestrator.
FASE 2	Optimizar	Días 15—45	Procesamiento con reconocimiento de aplicaciones, Backup Copy Jobs (Trabajos de copia de backup), nivel externo de Veeam Data Cloud Vault y configuración de Veeam Recovery Orchestrator (Premium).
FASE 3	Resiliencia de datos y resiliencia del negocio	Días 46—75	Cierre las brechas de cobertura, habilite Recon, preparación contra el ransomware, ajuste, y elabore planes de orquestación (Premium).
FASE 4	Demostrar valor	Días 76—100	Pruebas de recuperación orquestadas, generación de informes, documentación de la arquitectura e higiene continua.

Cómo usar esta guía

- Siga los hitos en orden. Avanzar antes de tiempo, especialmente hacia la configuración de Scale-out Backup Repository™ (SOBR) o Vault, antes de que sus repositorios locales y trabajos estén estables, genera brechas que suelen hacerse evidentes durante una restauración real.
- El cronograma es flexible. Los días son pautas, no plazos estrictos. Los entornos más pequeños pueden completar la fase 1 en menos de una semana. Los entornos más complejos pueden requerir más tiempo en fases posteriores.
- Use los puntos de decisión. Cuando surjan opciones de arquitectura (p. ej., ruta de implementación o estrategia de repositorio), haga una pausa, alinee a las partes interesadas y documente su decisión antes de continuar.
- Omita lo que no corresponde, pero anote el motivo. Si su edición no incluye Veeam ONE™ o Veeam Recovery Orchestrator, esos hitos estarán claramente marcados. De forma similar, los pasos de Veeam Software Appliance y Veeam Vault son opcionales y relevantes solo si esos módulos forman parte de su implementación.

Resumen de Veeam Data Platform

Antes de profundizar en la implementación y cómo llevarla a cabo, vamos a empezar con un resumen rápido de lo que incluye su Veeam Data Platform. Veeam Data Platform está disponible en tres ediciones, cada una de las cuales amplía la anterior:



Consulte el apéndice para las descripciones de todos los componentes: "Apéndice: Referencia rápida. Componentes fundamentales".

Tómese un momento para confirmar su edición.

Antes de continuar, confirme su edición y haga un inventario completo de lo que está incluido. En la protección de datos, las funcionalidades no utilizadas no son solo valor desperdiciado, sino brechas que esperan ser expuestas.

Además, los siguientes módulos están disponibles en todas las ediciones:

- **Veeam Software Appliance:** una plataforma de implementación pre-reforzada, sin Windows, que simplifica la configuración de la infraestructura y refuerza la postura de seguridad. No se requieren conocimientos de Linux.
- **Veeam Vault:** almacenamiento de backup inmutable off-site ofrecido como servicio para proteger tus datos frente al ransomware y el borrado accidental.
- **Veeam Agents:** los agentes de Veeam son agentes de software que ofrecen backups a nivel de imagen, backup y recuperación con la calidad de Veeam para servidores físicos, endpoints y plataformas de máquinas virtuales virtual (VM) no soportadas, gestionados de forma centralizada desde la consola de Veeam Backup & Replication.

El camino hacia la resiliencia comienza aquí.

Durante los próximos 100 días, avanzará desde la implementación hasta un entorno totalmente reforzado y recuperable de manera verificable, hito a hito, sin trabajo de averiguación.

FASE 1 **Base** **Días 1—14**	**FASE 2** **Optimizar** **Días 15—45**	**FASE 3** **Resiliencia de datos y resiliencia del negocio** **Días 46—75**	**FASE 4** **Demostrar valor** **Días 76—100**
M1: Dimensionamiento y planificación	M4: Procesamiento con reconocimiento de aplicaciones	M7: Cerrar las brechas de cobertura	M10: Pruebas de recuperación
M2: Despliegue de Veeam Software Appliance e infraestructura	M5: Copia de backup, SOBR y Vault	M8: Preparación para ransomware	M11: Informes y documentación
M3: Primeros trabajos de backup	M6: Monitorización, alertas y configuración de Orchestrator	M9: Ajustes de rendimiento y planes de orquestación	M12: Higiene continua

FASE 1 • Días 1—14

Base

Objetivo: infraestructura dimensionada, desplegada y primeras cargas de trabajo protegidas.

Hito 1: Dimensionamiento y planificación

Antes de desplegar cualquier cosa, invierta tiempo en el dimensionamiento. Una infraestructura infradimensionada es la causa más común de la lentitud de las ventanas de backup y del incumplimiento de los RPO en los primeros 100 días.

Inventario de cargas de trabajo

- Documente el número total de máquinas virtuales (VM) y cargas de trabajo, la huella de datos (total aprovisionado vs. utilizado) y la tasa de cambio diaria estimada.
- Identifique sus cargas de trabajo críticas, ya que estas determinan sus objetivos de RPO y RTO.
- Tenga en cuenta cualquier carga de trabajo física (por ejemplo, servidores Windows/Linux) que requiera Veeam Agents.

Dimensionamiento de Veeam Software Appliance

- Veeam Software Appliance se suministra con Veeam Backup & Replication preinstalado, por lo que su principal decisión de dimensionamiento es el host en el que se ejecuta.
- Mínimo para pequeñas y medianas empresas (PYMES): 8 vCPU / 16 GB de RAM (se recomienda 500 MB de RAM para cada trabajo simultáneo).
- Utilice la calculadora de dimensionamiento de Veeam (calculator.veeam.com) para validar los requisitos de recursos según la cantidad de cargas de trabajo y la huella de datos.
- Elija su formato de implementación: un OVA para VMware vSphere o un ISO para servidores físicos y otros hipervisores. De cualquier manera, no se requiere experiencia en Linux.

Arquitectura de almacenamiento: elija su camino

La elección de almacenamiento en esta etapa determina el resto de las Fases 1 y 2. Hay tres rutas recomendadas para PYME:

Ruta A: Veeam Software Appliance + Veeam Infrastructure Appliance como repositorio reforzado de Veeam. + Vault: esta es la configuración base recomendada. Esta ruta proporciona un repositorio local inmutable sin necesidad de conocimientos de Linux, además de copias inmutables, offsite y aisladas lógicamente mediante Vault.

Ruta A: ¿Por qué usar un repositorio reforzado de Veeam. implementado mediante Veeam Infrastructure Appliance?

Un repositorio reforzado de Veeam proporciona backups locales inmutables. Esto significa que el ransomware no puede cifrarlos ni eliminarlos durante el periodo de retención.

Tradicionalmente, un repositorio inmutable de Linux requiere un servidor Linux dedicado y el endurecimiento manual del OS. Veeam Infrastructure Appliance elimina esa barrera por completo. Veeam Infrastructure Appliance se proporciona pre-reforzado, se implementa desde un OVA o ISO y no requiere experiencia en Linux para ponerlo en marcha ni mantenerlo.

Veeam Infrastructure Appliance es un dispositivo de función única. Cada instancia opera como un repositorio reforzado de Veeam o un proxy de backup. Para las PYME sin un administrador de Linux dedicado o almacenamiento inmutable existente, el uso de un repositorio reforzado de Veeam proporcionado por Veeam Infrastructure Appliance es el camino recomendado hacia la inmutabilidad local.

Para obtener la máxima protección, implemente Veeam Infrastructure Appliance en hardware físico. Cuando se ejecuta Veeam Infrastructure Appliance como un dispositivo virtual, se sigue heredando la superficie de ataque del hipervisor. La inmutabilidad a nivel del sistema de archivos protege los archivos de backup contra ataques dentro del OS, pero un administrador del hipervisor aún puede eliminar las VM incluso si los archivos de backup son inmutables.

Ruta B: Veeam Software Appliance + Veeam Data Cloud Vault: Veeam Backup & Replication realiza backups directamente en el repositorio local en Veeam Software Appliance y mantiene una copia offsite en Veeam Vault. Esto es ideal para micro-PYMEs, sucursales o clientes que desean minimizar la gestión del almacenamiento local, además de contar con copias inmutables offsite y lógicamente aisladas a través de Vault. Tenga en cuenta que, si Veeam Software Appliance se implementa en una infraestructura virtual, no es un sustituto adecuado para inmutabilidad en el sitio.

Ruta B: ¿Por qué Veeam Software Appliance + Veeam Vault?

La ruta B mantiene la administración de almacenamiento al mínimo. Veeam Backup & Replication almacena los backups en un repositorio local en el propio Veeam Software Appliance, y luego un trabajo de copia de backup los replica offsite en Vault.

El almacenamiento local de Veeam Software Appliance es inmutable por defecto, por lo que la ruta B sigue brindándole protección contra ransomware en las instalaciones locales. No se trata de un repositorio reforzado de Veeam formal en el sentido del producto, por lo que la ruta A sigue siendo la alternativa más robusta cuando se dispone de hardware para dedicar a Veeam Infrastructure Appliance, pero la ruta B es la opción adecuada cuando no lo tiene. Al igual que con la Ruta A, Veeam Software Appliance ejecutándose como un appliance virtual aún puede ser eliminado en la capa del hipervisor, por lo que despliegue en hardware físico siempre que sea posible.

La ruta B omite por completo el paso de Veeam Infrastructure Appliance. Si elige esta ruta, proceda desde el Hito 2 (implementación de Veeam Software Appliance) directamente al Hito 5 (Backup Copy Jobs (Trabajos de copia de backup) a Vault).

Ruta C: Veeam Software Appliance + NAS/repositorio Windows existente + Vault o almacenamiento off-site de terceros alternativo: esta ruta aprovecha la infraestructura de almacenamiento existente y está menos reforzada localmente, a menos que se aplique una configuración adicional. Esto es útil cuando los clientes quieren aprovechar los socios existentes de Veeam Cloud & Service Provider (VCSP) para almacenamiento offsite o almacenamiento offsite alternativo que ya tienen disponible.

Independientemente de la ruta que elija:

- Considere aislar el tráfico de backup en una VLAN o NIC dedicada para mantener los datos de backup fuera de su red de producción.
- Revise la cobertura de licencias por socket/carga de trabajo antes de la implementación.

Hito 2: Despliegue de Veeam Software Appliance e infraestructura

Despliegue de Veeam Software Appliance

- Descargue el OVA de Veeam Software Appliance (para VMware vSphere) o el ISO (para servidores físicos o VM en otros hipervisores compatibles) desde el Portal para clientes de Veeam (my.veeam.com).
- Para OVA: importe en VMware vSphere y encienda. Veeam Backup & Replication se podrá acceder a través de la interfaz de administración después del primer inicio.
- Para ISO: inicie el servidor de destino (por ejemplo, físico o una VM en cualquier otro hipervisor compatible) desde la ISO y siga la Guía de configuración. Veeam Backup & Replication se instala automáticamente.
- Complete el asistente de configuración inicial de Veeam Software Appliance y establezca el nombre de host, la configuración de red y las credenciales de administrador.

Conecte la infraestructura a Veeam Backup & Replication

- Agregue su plataforma de virtualización al inventario de Veeam Backup & Replication (Infraestructura de backup > Servidores administrados).
- Agregue al menos un proxy de backup. En entornos más pequeños, Veeam Software Appliance puede servir como proxy inicial.
- Para entornos VMware, configure el modo de transporte Hot-Add. La VM proxy monta los discos de origen mediante SCSI y los lee directamente, evitando así la ruta NBD más lenta a través de la red de administración de ESXi.

Desplegar Veeam Infrastructure Appliance (Ruta A)

- Descargue el OVA o ISO de Veeam Infrastructure Appliance desde el Veeam Customer Portal.
- Despliegue usando el mismo procedimiento OVA/ISO que el de Veeam Software Appliance. Durante el asistente de configuración, seleccione "Repositorio reforzado" o "proxy de backup" como el rol de destino.
- Una vez implementado, agregue el Veeam Infrastructure Appliance a Veeam Backup & Replication como un servidor administrado, luego configúrelo como un repositorio de backup o proxy.
- Para el rol de repositorio reforzado, agregue el repositorio en Veeam Backup & Replication (Infraestructura de backup > Repositorios de backup) y establezca el período de retención de inmutabilidad.
- Omita esta sección si está utilizando la ruta B o la ruta C (ya que no se requiere Veeam Infrastructure Appliance).

Lo que Veeam Software Appliance gestiona para usted

Veeam Backup & Replication está preinstalado y listo para configurarse sin necesidad de configuración manual del OS, instalación de software o parches previos a la implementación.

Veeam Software Appliance viene pre-reforzado, los servicios innecesarios se deshabilitan, el OS está reforzado y se aplican las Mejores prácticas de seguridad por defecto.

Implemente como un OVA en VMware vSphere, arranque desde el ISO en un servidor físico o arranque dentro de una VM en cualquier otro hipervisor compatible con Veeam. No se necesita experiencia en Linux.

Instalar Veeam ONE

- Veeam ONE es un instalador independiente para Windows. Actualmente no se entrega como parte del modelo de appliance.
- Instale Veeam ONE en una VM de Windows Server o en un host físico (consulte los requisitos mínimos en la Guía de implementación de Veeam ONE).
- Conecte Veeam ONE a Veeam Backup & Replication y a su host vCenter/Hyper-V durante el asistente de configuración.
- Configure los ajustes de notificación SMTP/correo electrónico inmediatamente después de la instalación. Asegúrese de que las alertas estén activas desde el día 1.

Hito 3: Primeros trabajos de backup

- Cree su primer trabajo de backup para su hipervisor principal. Elija el repositorio reforzado de Veeam (ruta A), el repositorio local en Veeam Software Appliance (ruta B) o su repositorio NAS/Windows existente (ruta C).
- Establezca una política de retención razonable para comenzar: 14 puntos de restauración diarios, 4 semanales, 3 mensuales (GFS).
- Programe el trabajo para que se ejecute fuera de las horas pico y asegúrese de que no entre en conflicto con ningún periodo de mantenimiento.
- Realice la primera ejecución del trabajo manualmente y monitoree el proceso hasta completarlo.
- Verifique que el trabajo haya finalizado sin advertencias ni errores antes de pasar a la Fase 2.

Primera prueba de restauración : ¡no la omita!

Antes de pasar a la Fase 2, realice un Instant VM Recovery de una VM no crítica para confirmar la capacidad de recuperación.

No estará protegido hasta que haya verificado que puede restaurar. Esto toma minutos y puede prevenir días de problemas más adelante.

Qué gestiona Veeam Infraestructura Appliance por usted

Al igual que Veeam Software Appliance, Veeam Infrastructure Appliance se entrega reforzado y preconfigurado para su función asignada. No se requiere administración de Linux después de la implementación.

Un solo Veeam Infrastructure Appliance cumple una función: repositorio reforzado de Veeam o proxy de backup. Si necesita ambos, despliegue dos appliances.

Tiene los mismos formatos de implementación que Veeam Software Appliance: OVA para VMware vSphere o ISO para servidores físicos y otros hipervisores compatibles.

FASE 2 • Días 15—45

Optimizar

Objetivo: protección consistente, copia off-site y visibilidad en todo el entorno.

Hito 4: Procesamiento con reconocimiento de aplicaciones

El procesamiento con reconocimiento de aplicaciones garantiza que los backups coherentes frente a bloqueos también sean consistentes con las aplicaciones. Esto es fundamental para las cargas de trabajo transaccionales como las de SQL Server, Oracle, Exchange, Active Directory y otras cargas de trabajo aplicables.

- Habilite el procesamiento de invitados en los trabajos de backup que cubran servidores de aplicación de Windows o Linux.
- Configure el procesamiento con reconocimiento de aplicaciones para Servidor SQL, Oracle, Exchange, controladores de dominio de Active Directory (Directorio activo) y otras cargas de trabajo aplicables.
- Establezca una política de truncamiento del registro de transacciones cuando corresponda y apropiada para sus necesidades de recuperación.
- Después de la primera ejecución de un trabajo con reconocimiento de aplicaciones, confirme que los puntos de restauración estén marcados como consistentes con las aplicaciones en Veeam Backup & Replication.
- Realice una restauración a nivel de elementos de una base de datos SQL (o de otras cargas de trabajo aplicables) con Veeam Explorer for SQL Server para verificar que la recuperación de aplicación de extremo a extremo funciona.

Hito 5:
Copia de backup y Vault

Este hito completa su estrategia 3-2-1: una copia local en su repositorio primario, más una copia inmutable off-site. Este es el pilar arquitectónico de su entorno de backup.

Conectar Vault

- Añada Vault como un repositorio de almacenamiento de objetos en Veeam Backup & Replication (Infraestructura de backup > repositorios de almacenamiento de objetos).
- Autentique con sus credenciales emitidas por Veeam y seleccione su región.
- Confirme que la inmutabilidad está activada.

Trabajos de copia de backup

- Configure Backup Copy Jobs (Trabajos de copia de backup) con una política de retención GFS para mantener puntos de restauración a largo plazo offsite.
- Verifique que los trabajos de copia off-site se completen correctamente y confirme que los objetos de Vault muestran banderas de inmutabilidad en Veeam Backup & Replication.
- Realice una restauración de prueba desde Vault para confirmar que la copia off-site es legible antes de declarar la fase 2 como completa.

Ruta C: Opciones de destino offsite

Las rutas A y B utilizan Vault como destino para la copia off-site. La ruta C puede utilizar Vault o un VCSP alternativo, o un repositorio off-site de terceros si ya cuenta con uno. La inmutabilidad se aplica de forma predeterminada a todos los Datos de backup almacenados en Vault. Si utiliza un repositorio externo que no sea Vault, confirme que la inmutabilidad o el bloqueo de objetos estén configurados en ese repositorio.

Hito 6: Monitorización, alertas y configuración de Orchestrator

- Configure los destinatarios de las notificaciones de alarmas por correo electrónico en Veeam ONE: alertas por correo electrónico sobre errores en los trabajos y acuerdos de nivel de servicio (SLA) no cumplidos.
- Defina el horario laboral en Veeam ONE para alinear los cálculos de SLA con su programación operativa.
- Revise los umbrales de alarma predeterminados: deshabilite o ajuste las alarmas que no sean relevantes para su entorno para evitar la fatiga de alertas.
- Ejecute sus primeros informes de Veeam ONE: informe de VM protegidas e informe de sesiones de trabajo.
- Revise el informe de VMs sin protección y resuelva cualquier brecha identificada antes de avanzar a la Fase 3.

Instale Veeam Recovery Orchestrator (solo en la edición Premium)

Omita esta sección si su edición es Foundation o Advanced. Veeam Recovery Orchestrator se incluye únicamente con Veeam Data Platform Premium.

- Veeam Recovery Orchestrator es un instalador independiente basado en Windows. Puede alojarse junto con Veeam ONE™ en el mismo host de Windows o ejecutarse en su propio host.
- Instale Veeam Recovery Orchestrator en una VM de Windows Server o en un host físico. Consulte los requisitos mínimos en la Guía de implementación de Veeam Recovery Orchestrator.
- Durante el asistente de configuración, conecte Veeam Recovery Orchestrator a su instancia de Veeam Backup & Replication para que pueda realizar un inventario de sus cadenas de backup existentes.
- Conecte Veeam Recovery Orchestrator a su vSphere, Hyper-V o Microsoft Azure para que la ejecución planificada pueda encender las VM y asignar redes correctamente.
- Opcionalmente, conecte Veeam Recovery Orchestrator a Veeam ONE para obtener datos de monitorización más enriquecidos y verificación basada en DataLab.
- Aplique su licencia de Veeam Data Platform Premium para activar Veeam Recovery Orchestrator.
- Configure SMTP/email para que las notificaciones de ejecuciones planificadas funcionen desde el día 1.

FASE 3 • Días 46—75

Resiliencia de datos y del negocio

Objetivo: cerrar brechas de protección, mejorar los RTO/RPO y agregar resiliencia contra ransomware.

Hito 7: Cerrar las brechas de cobertura

- Ejecute el informe de VMs sin protección en Veeam ONE™ para abordar todas las cargas de trabajo sin protección antes de realizar cualquier otro ajuste.
- Extienda la protección a las cargas de trabajo físicas utilizando Veeam Agent *para Microsoft Windows* o Veeam Agent *para Linux*, según sea necesario.
- Revise las programaciones de trabajo en busca de conflictos y escalone las horas de inicio para evitar la contención de recursos proxy y repositorio.
- Valide el cumplimiento de RPO: ¿todas las VM críticas generan puntos de restauración dentro de su ventana objetivo de recuperación?
- Confirme que todos los trabajos se están completando dentro de la ventana de backup definida.

Añadir capacidad proxy con un segundo VIA

Si los trabajos de backup se están ejecutando lentamente o exceden su ventana de backup, implemente un segundo dispositivo de infraestructura de Veeam en función de proxy.

El modelo de dispositivo pre-reforzado hace que esto sea rápido: implemente el OVA o ISO, regístrelo en Veeam Backup & Replication, y los trabajos equilibrarán automáticamente la carga entre ambos proxies sin necesidad de configuración manual del proxy.

Hito 8: Preparación para el ransomware

- Veeam Data Platform Advanced y Premium se suministran con dos herramientas de seguridad complementarias. El primero es Recon, el servicio de inteligencia de amenazas de Veeam que identifica indicadores de compromiso (IOC) y datos emergentes extraídos de la respuesta a incidentes reales. La segunda es el escaneo de backup, una acción integrada en el producto Veeam Backup & Replication. Analiza las cadenas de backup existentes en busca de indicadores de malware y valida la integridad de los archivos, sin requerir una red aislada ni iniciar VMs.

Ejecute un escaneo de backup:

- Cree un trabajo de SureBackup en Veeam Backup & Replication en Inicio > SureBackup. SureBackup se ejecuta como un trabajo programado y puede analizar sus backups en busca de malware, amenazas basadas en firmas y la integridad de archivos en un único flujo de trabajo, sin requerir una red aislada ni el arranque de una VM para el análisis.

- Vincule los trabajos de backup que desea cubrir, de modo que con el tiempo el trabajo de SureBackup abarque todos sus datos: repositorio reforzado de Veeam (Ruta A), repositorio local de Veeam Software Appliance (Ruta B), repositorio NAS/Windows existente (Ruta C) y Vault.
- En las opciones de verificación, habilite el escaneo de malware con Veeam Threat Hunter (o una solución antivirus de terceros) para verificar el contenido del backup contra una base de datos actualizada de Firmas de amenazas.
- En las mismas opciones de verificación, habilite la comprobación de integridad del archivo para validar el archivo de backup mediante una comprobación CRC y así identificar bloques corruptos.
- Programe el trabajo de SureBackup® y revise los resultados de la sesión con regularidad; investigue cualquier punto de restauración marcado antes de usarlos para la recuperación.
- Para una comprobación puntual entre ejecuciones programadas, vaya a Inicio > Backups, expanda el trabajo de backup, seleccione la carga de trabajo y elija Analizar backup desde la pestaña backup.

Instale Recon

- Instale el binario de Recon en cualquier host de infraestructura Veeam basado en Windows o en cualquier host Linux de su elección.
- Recon también se puede instalar en los controladores de dominio de Windows aplicables.
- Recon no puede instalarse en Veeam Infrastructure Appliance. Los dispositivos de infraestructura de Veeam son individuales y están pre-reforzados.

Auditoría de inmutabilidad

- Confirme que el período de inmutabilidad en el repositorio reforzado de su Veeam Infrastructure Appliance esté configurado con una ventana de retención adecuada.
- Revise la configuración de cifrado de backup y habilite el cifrado en el destino en los trabajos si aún no está configurado.
- Ejecute el informe "Cargas de trabajo inmutables" de Veeam ONE para medir e identificar los objetivos de inmutabilidad de backup de cargas de trabajo.

Preparación para la recuperación de ransomware

Documente un runbook sencillo de recuperación que incluya qué VM restaurar primero, desde qué puntos de restauración y hacia qué destino.

Identifique al menos un punto de restauración limpio, previo a la infección, en Vault como su último punto de referencia conocido.

Sus copias inmutables no pueden sobrescribirse ni cifrarse durante el periodo de inmutabilidad. Esta es su red de seguridad.

Ruta A: repositorio reforzado de Veeam más Vault.

Ruta B: almacenamiento local de la Veeam Software Appliance más Veeam Vault.

Ruta C: Vault más su repositorio local si ha configurado la inmutabilidad allí.

Hito 9: Ajustes de rendimiento y planes de orquestación

- Revise el rendimiento del proxy en las estadísticas de trabajo de Veeam Backup & Replication. Si los trabajos tienen cuellos de botella, implemente un segundo dispositivo de infraestructura de Veeam en el rol de proxy.
- Confirme que el modo de transporte de backup es óptimo: Hot-Add (VMware) o Acceso directo al almacenamiento donde esté disponible.
- Asegúrese de que todos los trabajos de backup estén completos dentro de su ventana de mantenimiento definida.
- Revise las gráficas de rendimiento de Veeam ONE™ e identifique las máquinas virtuales con tasas de cambio inusualmente altas que puedan beneficiarse de trabajos dedicados o de ajustes en los horarios.

Cree planes de orquestación inicial (solo para la edición Premium)

Omita esta sección si su edición es Foundation o Advanced, o si no está utilizando un hipervisor compatible con Veeam Recovery Orchestrator.

Veeam Recovery Orchestrator convierte su runbook de recuperación manual en un plan ejecutable. Crear planes ahora significa que la Fase 4 puede verificar la capacidad de recuperación automáticamente en lugar de volver a ejecutar restauraciones manuales.

- Identifique las pilas de aplicaciones de nivel 1 (tier-1) que requieren recuperación orquestada (p. ej., controladores de dominio, base de datos principal, servidores de aplicaciones principales).
- En Veeam Recovery Orchestrator, cree su primer plan de restauración para una de esas pilas.
- Defina el orden de arranque de las VMs y sus dependencias para que los requisitos previos (por ejemplo, DCs, DNS, etc.) estén disponibles antes que los servicios dependientes.
- Configure los objetivos de recuperación (p. ej., host, clúster, almacén de datos) y mapee la red de producción para el failover real, y una red aislada para pruebas.
- Establezca los objetivos RTO y RPO del plan para que Veeam Recovery Orchestrator pueda marcar las desviaciones con el tiempo.
- Guarde el plan y revise la documentación generada automáticamente con las partes interesadas antes de declarar que la Fase 3 se ha completado.

Fase 4 • Días 76—100

Demostrar valor y operacionalizar

Objetivo: verificar la capacidad de recuperación, establecer una higiene continua y demostrar el ROI.

Hito 10: Pruebas de recuperación

La única backup que importa es aquella de la que pueda restaurar. La fase 4 es donde se demuestra — con evidencia documentada — tque su entorno cumple con sus compromisos de RTO y RPO.

SureBackup y escaneo de backup

- Configure un grupo de aplicaciones de SureBackup que cubra sus VM más críticas (p. ej., controladores de dominio, servidores de aplicaciones clave).
- Ejecute un trabajo de SureBackup para automatizar la verificación de arranque y confirmar que las VMs inicien y pasen las pruebas de latido, ping y a nivel de aplicación.
- Para una verificación más ligera, ejecute un Scan Backup. Valida la integridad de los archivos y comprueba amenazas sin arrancar las VMs, lo que constituye un complemento práctico o una alternativa a SureBackup en entornos más pequeños.

Pruebas de restauración completa y restauración granular

- Pruebe restauraciones a nivel de archivo y recupere archivos individuales de un backup a una ubicación de prueba.
- Pruebe la recuperación de elementos de aplicación restaurando un objeto de base de datos SQL o un usuario de Active Directory mediante Veeam Explorers.
- Pruebe una restauración de VM completa desde Vault para simular la pérdida total en las instalaciones locales y validar su copia off-site.
- Registre los tiempos de recuperación reales, compárelos con sus objetivos de RTO y documente los resultados.

Mejores prácticas para las pruebas de recuperación

Siempre restaure en un entorno fuera de producción y nunca sobrescriba cargas de trabajo en funcionamiento durante una prueba.

Documente qué se restauró y desde qué punto de restauración, a qué destino y cuánto tiempo tardó.

Estos resultados son la prueba de la capacidad de recuperación. Guárdelos para revisiones de cumplimiento normativo, auditorías e informes de gestión.

Ejecute planes de orquestación (solo edición Premium)

Omita esta sección si su edición es Foundation o Advanced, o si su hipervisor no es compatible con Veeam Recovery Orchestrator. La fase 3 construyó su primer plan de restauración, pero la fase 4 es donde demuestra su verdadero valor.

- Ejecute una prueba de preparación sin supervisión en su plan. Veeam Recovery Orchestrator verifica la disponibilidad de los puntos de restauración, la capacidad del destino y la desviación de configuración, sin tener que arrancar ninguna VM.
- Ejecute una prueba de DataLab en su plan. Veeam Recovery Orchestrator restaura la pila de aplicaciones en una red aislada y realiza comprobaciones a nivel de aplicación sobre VM en funcionamiento.
- Registre los tiempos de recuperación reales de la ejecución del DataLab y compárelos con el objetivo de RTO que estableció en la Fase 3.
- Genere el informe de preparación para la recuperación de Veeam Recovery Orchestrator y archívelo junto con los demás resultados de las pruebas de recuperación.
- Para las cargas de trabajo que no estén cubiertas por un plan de Veeam Recovery Orchestrator, recurra a las pruebas de restauración manual mencionadas anteriormente.

Hito 11: Informes y documentación

Genere un informe mensual de Resumen ejecutivo de Veeam ONE™ y compártalo con la gerencia para demostrar el estado de backup y la cobertura del backup.

- Genere un informe de inventario de cargas de trabajo protegidas para confirmar el alcance de la cobertura.
- Documente su arquitectura final de backup, incluyendo la lista de trabajos, el diseño del repositorio, los roles de Veeam Infrastructure Appliance, las programaciones y las políticas de retención.
- Revise el consumo de almacenamiento de Veeam Vault y asegúrese de que su uso se corresponda con su presupuesto previsto.
- Archive los resultados de las pruebas de recuperación junto con la documentación de la arquitectura.
- Solo en la versión Premium: genere el informe de preparación para la recuperación de Veeam Recovery Orchestrator cada mes. Monitoree la puntuación de preparación a lo largo del tiempo a medida que cambian las cargas de trabajo y las dependencias.
- Solo en la versión Premium: archive la documentación del plan generada por Veeam Recovery Orchestrator junto con sus documentos de arquitectura. Veeam Recovery Orchestrator regenera la documentación automáticamente cuando se actualizan los planes; archívela de nuevo cada vez que se actualicen los planes.

Hito 12:
Cadencia de higiene continua

Para el día 100, su entorno debería estar estable y completamente documentado. Con estos hábitos, se mantendrá de esa manera:

- **Semanalmente:** revise su panel de control del estado del trabajo de Veeam ONE y aborde rápidamente los errores o advertencias.
- **Semanalmente:** revise el informe de VMs sin protección en Veeam ONE™ y agregue cobertura para cualquier nueva VM.
- **Mensualmente:** realice un resumen ejecutivo e informes de VM protegidas y comparta los resultados.
- **Mensualmente:** revise el consumo de almacenamiento de Vault y la tasa de crecimiento. Indique si está superando su huella presupuestada o si se acercan próximos aumentos de retención.
- **Mensualmente:** confirme que las ventanas de retención siguen activas y sin modificaciones.
- **Trimestralmente:** realice una prueba de recuperación documentada y alterne los tipos de carga de trabajo.
- **Trimestralmente:** ejecute un escaneo de backup en cada repositorio para verificar Firmas de malware y deriva de integridad de archivos.
- **Trimestralmente:** revise quién tiene acceso administrativo a Veeam Backup & Replication, Veeam ONE y Veeam Recovery Orchestrator (solo para la versión Premium). Elimine el acceso a cualquier persona que haya cambiado de rol o se haya ido.
- **Trimestral (solo Premium):** ejecute un test de Veeam Recovery Orchestrator DataLab y alterne qué plan de orquestación se ejercita.
- **Trimestral (solo Premium):** regenere y archive la documentación del plan de Veeam Recovery Orchestrator si algún plan ha cambiado desde la última revisión.
- **Mensualmente:** revise las actualizaciones de inteligencia sobre amenazas de Recon y aplique las firmas o reglas pertinentes a su entorno.

- **Anualmente:** revise su arquitectura de backup y políticas de retención según los requisitos empresariales actuales y las nuevas obligaciones de cumplimiento.

- **Anualmente:** realice una restauración completa desde Vault para validar que la copia off-site sea recuperable de extremo a extremo. Documentar el resultado.

- **Anualmente:** revise la configuración de cifrado durante la copia y en el destino, y rote las claves según su política de seguridad.

- **Según sea necesario:** planifique la cadencia de actualización de los componentes de Veeam (por ejemplo: Veeam Software Appliance, Veeam Infraestructura Appliance, Veeam ONE™, Veeam Agents y Veeam Recovery Orchestrator, si corresponde) y suscríbase a las notificaciones sobre nuevas versiones.

- **Antes de la renovación:** revise el uso de las licencias, las proyecciones de crecimiento y la adecuación de la edición. Si has superado el conjunto de características de tu edición, este es el momento de hablar sobre una actualización con tu representante de Veeam.

Recomendaciones finales

¡Enhorabuena! ¡Lo logró!

En 100 días, implementó y puso en marcha un entorno de protección de datos totalmente operativo. Sus cargas de trabajo están protegidas, sus backups están reforzados e inmutables, y ha demostrado que puede recuperar no solo en teoría, sino con pruebas.

Eso no es poca cosa.

Ahora el enfoque pasa de la implementación al mantenimiento. Mantenga las restauraciones en un programa de pruebas regular, ajuste las políticas a medida que evoluciona su entorno y utilice su cadencia de monitorización y generación de informes para detectar desviaciones antes de que se conviertan en riesgos. Los hábitos que usted estableció en el Hito 12 — su cadencia de higiene semanal, mensual, trimestral y anual — son los que mantienen su entorno íntegro mucho después del Día 100. Sígalos, adóptelos y evoluciónelos a medida que su organización crezca.

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

Mantenga sus roles de administrador al día para que las personas correctas tengan el acceso apropiado, y permanezca suscrito a las notas de la versión y avisos de seguridad de Veeam para estar siempre informado.

No tiene que hacer esto solo

Las comunidades, recursos de aprendizaje y equipos técnicos de Veeam existen para ayudarle a llegar más lejos. ¡Aprovéchelos a medida que su entorno crece y madura! Una lista seleccionada de recursos está disponible en el apéndice.

Si tiene preguntas o necesita ayuda con los próximos pasos, comuníquese con su gerente de cuentas de Customer Success o contacte soporte técnico de Veeam para consultas técnicas.

Apéndice: Referencia rápida

Componentes clave: Veeam Data Platform

- **Veeam Software Appliance:** un dispositivo reforzado con Veeam Backup & Replication preinstalado. Despliegue como OVA (VM) o ISO (físico). Este es el punto de partida recomendado para todas las implementaciones de PYME.
- **Veeam Infrastructure Appliance:** un dispositivo preconfigurado y reforzado, desplegado como proxy de backup dedicado o repositorio reforzado. Proporciona inmutabilidad local sin necesidad de conocimientos de Linux, con un rol por appliance.
- **Veeam Backup & Replication:** un motor central de backup, alojado en Veeam Software Appliance. Gestiona trabajos, repositorios, proxies y operaciones de recuperación.
- **Veeam ONE:** realiza monitorización, alertas e informes. Tiene una instalación independiente basada en Windows y se conecta a Veeam Backup & Replication y a tu hipervisor para una visibilidad completa de toda la pila.
- **Recon:** este es el servicio de inteligencia de amenazas de Veeam. Identifica y muestra indicadores de compromiso (IOC), firmas de amenazas y datos de campañas emergentes obtenidos de respuestas a incidentes reales. Incluido con Veeam Data Platform Advanced.
- **Escanear el contenido de los backup:** esta es una acción dentro del producto que examina las cadenas de backup existentes para detectar firmas conocidas de malware y verificar la integridad de los archivos, sin requerir una red aislada ni iniciar VM. Incluido con Veeam Data Platform Advanced.
- **Veeam Recovery Orchestrator:** una plataforma de orquestación que automatiza la recuperación ante desastres (DR) a nivel de aplicación. Le permite crear planes de restauración ejecutables, realizar pruebas de preparación, efectuar verificaciones basadas en DataLab y generar documentación de recuperación. Incluido con Veeam Data Platform Premium.
- **Veeam Data Cloud Vault:** brinda almacenamiento de objetos en la nube inmutable para copias offsite. Es administrado por Veeam sin necesidad de una cuenta de nube independiente.

Términos clave

- **Objetivo de punto de recuperación (RPO):** pérdida de datos máxima aceptable, medida en tiempo. Determina la frecuencia de la Programación del backup.
- **Objetivo de tiempo de recuperación (RTO):** tiempo de inactividad máximo aceptable antes de que una carga de trabajo deba ser recuperada.
- **Grandfather-Father-Son (GFS):** esquema de retención que mantiene los puntos de restauración diarios, semanales y mensuales.
- **Inmutabilidad:** datos de backup que no pueden modificarse ni eliminarse durante un periodo de retención definido. Protege contra el cifrado por ransomware de los archivos de backup.
- **Instant VM Recovery:** restaura una VM directamente desde un backup en segundos, sin necesidad de copiar los datos previamente. Siempre migre al almacenamiento de producción después de la validación.
- **Plan de orquestación (Veeam Recovery Orchestrator):** un runbook ejecutable que define el orden, las dependencias, las ubicaciones de destino y las asignaciones de red para restaurar un conjunto de cargas de trabajo. Sustituye un runbook de recuperación manual por una automatización autodocumentada y verificable.
- **DataLabs:** un entorno de prueba aislado en el que Veeam Recovery Orchestrator (o SureBackup) restaura un backup y ejecuta la verificación a nivel de aplicación sin afectar la Producción. Permite realizar pruebas completas de planes con cualquier frecuencia.
- **Procesamiento con reconocimiento de aplicaciones:** procesamiento en máquinas invitadas que crea puntos de Backup consistente con las aplicaciones para Servidor SQL, Oracle, Exchange, Active Directory (Directorio activo), SharePoint, PostgreSQL y MySQL. Utiliza VSS en Windows y secuencias de comandos de pre-freeze y post-thaw, además de quiescencia nativa de la base de datos en Linux.
- **Repositorio reforzado de Veeam:** un repositorio de backups basado en Linux con inmutabilidad aplicada a nivel del sistema de archivos. Veeam Infrastructure Appliance ofrece un repositorio reforzado de Veeam preconfigurado sin necesidad de administración de Linux. El almacenamiento de objetos y el bloqueo de objetos son mecanismos de inmutabilidad separados, no repositorios reforzados de Veeam. La inmutabilidad a nivel de sistema de archivos protege contra ataques dentro del OS, pero no contra la destrucción a nivel de VM. Un repositorio reforzado de Veeam ejecutándose como un appliance virtual se puede eliminar aún en la capa del hipervisor, por lo que se recomienda implementar Veeam Infrastructure Appliance en hardware físico para obtener la máxima protección.
- **Modo de transporte Hot-Add:** es un método de transporte de backup específico de VMware. La VM proxy utiliza el modo Hot-Add para agregar los discos virtuales de la VM de origen y los lee mediante SCSI, evitando la ruta NBD sobre la red de administración ESXi.

Apéndice: Enlaces útiles

Mi cuenta

Su cuenta de Veeam es su centro de gestión para administrar su implementación. Una vez que haya iniciado sesión, puedes descargar productos y claves de licencia, gestionar administradores de casos, contactar con el Soporte de Veeam y renovar contratos o agregar licencias.

- Inicie sesión o cree una cuenta de Veeam
- Cómo crear una cuenta
- Preguntas frecuentes sobre el inicio de sesión
- Gestión de roles de administrador de licencias y/o de casos

Documentación y descargas

- Centro de ayuda con documentación técnica, guía de implementación y guía de usuario
- Descargas de productos, incluyendo actualizaciones de software, parches y Notas de la versión
- Base de datos de conocimientos de soporte con problemas comunes, pasos para la Resolución de problemas y soluciones recomendadas, actualizada periódicamente por los equipos de Soporte de Veeam e ingeniería de Veeam.

Aprendizaje y mejores prácticas

- Webinars de incorporación en vivo: webinars periódicos en los que puede hacer preguntas en tiempo real y escuchar directamente a los especialistas técnicos
- Veeam University FREE: Cursos autodidactas y certificaciones sin costo
- Calculadoras de dimensionamiento de Veeam: herramienta de estimación y dimensionamiento en línea utilizada para calcular los requisitos de infraestructura, almacenamiento y capacidad para las implementaciones de Veeam
- Mejores prácticas de diseño y configuración de infraestructura elaboradas por arquitectos de soluciones de Veeam: extraídas de implementaciones reales, que conviene revisar a medida que su entorno madura
- Indicaciones prácticas para Veeam Intelligence: colección seleccionada de indicaciones efectivas para ayudarlo a aprovechar todo el potencial de Veeam Intelligence
- Veeam Search: el portal de búsqueda centralizado de Veeam para acceder a los recursos de Veeam desde un solo punto

Comunidades Veeam

- Foros de la comunidad de Veeam: conéctese con sus colegas, comparta las mejores prácticas, asista a grupos de usuarios y eventos de la comunidad, y discuta casos de uso del mundo real
- Foros de I+D de Veeam: su línea directa con I+D de Veeam para discusiones sobre productos, preguntas técnicas y comentarios sobre características

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 en todo el mundo, incluyendo al 82% de las empresas Fortune 500.

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