



SuperTransporte



PLAN INSTITUCIONAL

BC/DR

Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR)

Lineamientos técnicos, operativos y normativos para la protección, respaldo, continuidad y recuperación de servicios soportados por Veeam Backup y appliance de 200 TB

Tipo de documento

Plan institucional de continuidad del negocio y recuperación ante desastres

Base tecnológica

Veeam Backup con almacenamiento de copias en appliance de 200 TB

Fecha de emisión

18 de marzo de 2026

⚠ Propósito del documento: establecer los lineamientos de gobierno, protección, respaldo, verificación, recuperación y mejora continua para asegurar la disponibilidad e integridad de la información y de los servicios críticos frente a incidentes operativos, fallas de infraestructura y eventos de ciberseguridad.

Documento elaborado con enfoque de continuidad, resiliencia operativa, seguridad de la información y buenas prácticas de recuperación verificable.

Contenido del documento

Secciones 1 – 8

1. Resumen ejecutivo

2. Introducción

3. Objetivos

4. Justificación

5. Metodología

6. Marco normativo y de referencia

7. Gobierno del BC/DR y responsabilidades

8. Estrategia institucional de backup y recuperación

Secciones 9 – 15

9. Configuración recomendada para Veeam Backup y appliance de 200 TB

10. Verificación de integridad, pruebas y simulacros

11. Activación del plan y recuperación operativa

12. Indicadores, seguimiento y mejora continua

13. Conclusiones

14. Recomendaciones finales

15. Referencias

Nota de enfoque

Alcance y base de referencia del documento

- Este documento se redacta como base formal de un plan BC/DR institucional y asume como punto de partida la existencia de Veeam Backup y un appliance local de 200 TB para almacenamiento de copias. Por tanto, además de describir la situación actual, incorpora lineamientos de madurez, seguridad y resiliencia recomendados por NIST, ISO, CISA, MinTIC y la documentación oficial de Veeam para que el esquema de respaldo no se limite a "tener copias", sino que garantice recuperación verificable y continuidad real.



Madurez y seguridad

Lineamientos de madurez, seguridad y resiliencia recomendados por NIST, ISO, CISA y MinTIC.



Base tecnológica

Veeam Backup y appliance local de 200 TB como punto de partida del esquema de respaldo.



Recuperación verificable

El esquema de respaldo no se limita a "tener copias", sino que garantiza recuperación verificable y continuidad real.

1. Resumen ejecutivo

La continuidad del negocio y la recuperación ante desastres no deben entenderse únicamente como un conjunto de copias de seguridad, sino como una capacidad institucional para sostener o restablecer procesos críticos cuando se presentan incidentes de ciberseguridad, fallas tecnológicas, errores humanos, indisponibilidad de infraestructura, pérdida de datos o eventos externos de alto impacto. En ese sentido, el presente plan adopta una visión integral de resiliencia operativa, articulando gobierno, riesgos, protección, recuperación y mejora continua. La guía de NIST para la planeación de contingencia indica que la organización debe comprender el propósito, el proceso y la estructura del plan de contingencia, y relacionarlo con la resiliencia organizacional y el ciclo de vida de los sistemas [Ref. R1].

Desde el punto de vista de capacidad tecnológica, la organización cuenta con Veeam Backup y con un appliance de 200 TB destinado al almacenamiento de respaldos. Esta condición ofrece una base importante para la protección de activos de información, pero por sí sola no garantiza una postura robusta de recuperación. Para que el entorno sea realmente confiable, las copias deben contar con diseño por criticidad, retenciones definidas, protección frente a alteración o borrado, verificación de integridad, controles de acceso, cifrado, monitoreo continuo y pruebas de restauración periódicas. CISA insiste en que los respaldos deben mantenerse cifrados, desconectados u offline cuando corresponda, y probarse regularmente en escenarios de recuperación [Ref. R3].

Con fundamento en lo anterior, este documento propone una arquitectura de continuidad y recuperación alineada con el enfoque 3-2-1-1-0, el cual, en las guías oficiales de Veeam, implica mantener al menos tres copias de los datos, en dos medios diferentes, una copia fuera del sitio, una copia offline/air-gapped o inmutable, y cero errores en la verificación de recuperación [Ref. R9, R10]. Asimismo, incorpora criterios de RTO y RPO, lineamientos de hardening, uso de Health Check, pruebas con SureBackup, análisis de seguridad de la infraestructura de respaldo y procedimientos de activación del plan. El objetivo final es que la plataforma de backup se convierta en un habilitador real de continuidad y no en un simple repositorio de archivos de respaldo.

3 copias

Al menos tres copias de los datos

2 medios

En dos medios diferentes

1 off-site

Una copia fuera del sitio

1 offline

Una copia offline, air-gapped o inmutable

0 errores

Cero errores en la verificación de recuperación

2. Introducción

La dependencia creciente de la operación institucional respecto de sistemas de información, bases de datos, plataformas de autenticación, servicios virtualizados, repositorios documentales y canales digitales obliga a que la protección de la información se gestione desde una perspectiva preventiva y de recuperación. Una organización puede tener múltiples controles de seguridad y aun así verse afectada por eventos disruptivos. Por esa razón, el BC/DR constituye una disciplina necesaria para asegurar que, incluso cuando los controles preventivos fallen o el incidente supere la capacidad de contención inicial, exista un camino documentado y probado para sostener o reanudar la operación.

ISO 22301 define la continuidad del negocio como un sistema de gestión documentado que permite a las organizaciones planificar, establecer, implementar, operar, supervisar, revisar, mantener y mejorar continuamente su capacidad para protegerse contra incidentes disruptivos, reducir su probabilidad y garantizar la recuperación [Ref. R5].

En paralelo, ISO/IEC 27001 exige integrar la seguridad de la información dentro de un proceso formal de gestión del riesgo, preservando la confidencialidad, integridad y disponibilidad de la información [Ref. R6]. El plan aquí propuesto recoge ambos enfoques y los adapta a un contexto práctico de respaldo y recuperación basado en Veeam.

En Colombia, la construcción de un esquema BC/DR también responde a obligaciones y lineamientos de política pública. El MSPI de MinTIC orienta a las entidades para que incorporen la seguridad de la información en procesos, trámites, servicios, sistemas e infraestructura, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos [Ref. R7]. La Resolución 500 de 2021 y su actualización posterior fortalecen el marco de seguridad digital, mientras que la Directiva Presidencial 02 de 2022 ordena contar con planes de continuidad del negocio y realizar ejercicios para probar su efectividad frente a la materialización de riesgos de seguridad de la información [Ref. R11, R12, R13].

Bajo esta perspectiva, el presente documento amplía la discusión desde el simple respaldo hacia un modelo operativo completo. Se describe cómo debe clasificarse la información, qué respaldar, con qué frecuencia, dónde conservarlo, cómo verificar la consistencia de los puntos de restauración, cuándo probar restauraciones, qué hacer ante corrupción o sospecha de malware, qué métricas revisar y cómo escalar una declaración formal de desastre. El texto tiene un propósito práctico y de gestión: servir como base formal para adopción institucional, auditoría, mejora continua y fortalecimiento técnico del esquema actual.

3. Objetivos

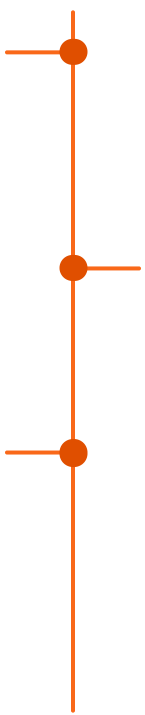
3.1 Objetivo general

Establecer un Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR) que permita proteger, respaldar, verificar, restaurar y recuperar de forma controlada la información y los servicios críticos de la organización, utilizando Veeam Backup y el appliance de 200 TB como elementos centrales de la estrategia, bajo criterios técnicos, operativos, regulatorios y de mejora continua.

3.2 Objetivos específicos

Definir lineamientos de continuidad y recuperación para los servicios, procesos y activos de información críticos de la organización, con criterios diferenciales según impacto y prioridad operativa.

Formalizar roles, responsabilidades, controles y frecuencias de operación para la ejecución, monitoreo, verificación y restauración de backups.



Establecer una estrategia de respaldo robusta, segura y verificable, alineada con buenas prácticas de NIST, ISO, CISA y Veeam, superando el enfoque limitado de mera generación de copias.

Incorporar prácticas de hardening, cifrado, inmutabilidad, segregación y verificación periódica de integridad para proteger los respaldos frente a fallas, errores y ataques de ransomware.

Alinear el esquema BC/DR con las referencias regulatorias colombianas aplicables y con estándares internacionales de continuidad y seguridad de la información.

Definir un marco de pruebas y simulacros que demuestre la capacidad real de recuperación y permita medir el cumplimiento de los tiempos objetivos de recuperación (RTO) y de los puntos objetivos de recuperación (RPO).

4. Justificación

La justificación principal de este plan radica en la necesidad de reducir el impacto operacional, económico, reputacional y jurídico derivado de la indisponibilidad de servicios o de la pérdida de información. En organizaciones intensivas en tecnología, la interrupción de una base de datos, un directorio de autenticación, una plataforma misional o un repositorio documental puede detener la prestación del servicio, afectar la toma de decisiones, comprometer obligaciones contractuales y deteriorar la confianza de usuarios internos y externos. Un BC/DR bien diseñado disminuye esa exposición porque establece capacidades previas de preparación, contingencia y restauración.

La existencia de Veeam Backup y de un repositorio de 200 TB representa una inversión relevante y útil, pero también implica responsabilidades de diseño y operación. Un repositorio amplio puede almacenar grandes cantidades de información, pero si no existen criterios claros de priorización, retención, verificación y seguridad, ese almacenamiento se convierte en un riesgo silencioso: puede llenarse con copias redundantes, inconsistentes, no probadas o vulnerables frente a modificación maliciosa. El objetivo del presente plan es transformar esa capacidad de almacenamiento en una plataforma gobernada, medible y recuperable.

También existe una justificación normativa. El MSPI establece un ciclo PHVA para la seguridad de la información y exige planificación, implementación, evaluación y mejoramiento continuo [Ref. R8]. La Directiva 02 de 2022 indica expresamente que deben existir planes de continuidad orientados al diagnóstico inicial, contención, respuesta, recuperación, reanudación y restauración, acompañados de ejercicios que permitan validar la efectividad del plan [Ref. R12]. Además, la Ley 1581 de 2012 obliga a proteger adecuadamente los datos personales y la Ley 1273 de 2009 refuerza la protección penal de la información y de los datos [Ref. R14, R15]. En consecuencia, la organización no solo necesita backups: necesita capacidad demostrable de recuperación segura.

5. Metodología

La metodología del presente plan se estructura sobre cinco ejes: análisis de impacto al negocio, valoración del riesgo, diseño de la estrategia de recuperación, implementación de controles técnicos y verificación periódica de la recuperabilidad. Este enfoque resulta coherente con NIST SP 800–34 Rev.1, que plantea una planeación de contingencia conectada con la resiliencia organizacional, el ciclo de vida del sistema y la gestión general de continuidad [Ref. R1]. Asimismo, es compatible con el enfoque de mejora continua exigido por ISO 22301 y por el MSPI [Ref. R5, R8].



En primer lugar, la metodología parte de la identificación de procesos críticos y de la determinación del impacto que generaría la interrupción de cada servicio. Esta etapa debe apoyarse en un BIA. La guía ISO/TS 22317 señala que la organización debe implementar y mantener un proceso formal y documentado de análisis de impacto al negocio apropiado a sus necesidades [Ref. R16]. A partir de este ejercicio se deben definir prioridades, dependencias técnicas, ventanas de recuperación y tolerancias de pérdida de datos.

En segundo lugar, se diseña la estrategia de respaldo y recuperación según criticidad. Esto implica decidir qué se respalda, con qué frecuencia, durante cuánto tiempo, en qué repositorios, bajo qué controles de seguridad y con qué método de restauración. La metodología evita el error de aplicar una única política genérica a todos los sistemas. En su lugar, propone segmentar por clases de servicio, sensibilidad de la información, criticidad del proceso y requisitos de disponibilidad.

En tercer lugar, se implementan controles técnicos sobre la plataforma de backup: cifrado, segmentación, hardening del repositorio, administración de privilegios, verificación de integridad, protección frente a ransomware, monitoreo de eventos y pruebas automatizadas o controladas de restauración. Finalmente, se establece un ciclo de evaluación y mejora continua, con indicadores, revisión de resultados, acciones correctivas y actualización periódica del documento cada vez que existan cambios de infraestructura, amenazas, lecciones aprendidas o hallazgos de auditoría.

6. Marco normativo y de referencia

El presente documento adopta como marco internacional principal la NIST SP 800–34 Rev.1, la cual orienta el desarrollo de planes de contingencia para sistemas de información; el NIST Cybersecurity Framework 2.0, que estructura la gestión del riesgo en las funciones Govern, Identify, Protect, Detect, Respond y Recover; ISO 22301 como estándar de continuidad del negocio; ISO/IEC 27001 como estándar base de gestión de seguridad de la información; e ISO/TS 22317 como guía para análisis de impacto al negocio [Ref. R1, R2, R5, R6, R16].

En el plano nacional, el plan toma como referencias prioritarias el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC; la Resolución 500 de 2021, que establece lineamientos y estándares para la estrategia de seguridad digital y adopta el MSPI; la actualización del Anexo 1 realizada en 2025 y las disposiciones de fortalecimiento asociadas a la evolución de riesgos como ransomware; la Directiva Presidencial O2 de 2022; y el Decreto 338 de 2022, que fortalece la gobernanza de la seguridad digital y articula prevención, detección, respuesta, recuperación y aprendizaje [Ref. R7, R8, R11, R12, R13].

Adicionalmente, se consideran como referentes jurídicos transversales la Ley 1581 de 2012 de protección de datos personales, la Ley 1273 de 2009 sobre protección de la información y de los datos, la Ley 1712 de 2014 sobre acceso a la información pública, y el Decreto 1078 de 2015 como marco general del sector TIC [Ref. R14, R15, R17, R18]. Estas normas no sustituyen el diseño técnico del backup, pero sí condicionan la forma en que deben tratarse los datos, la disponibilidad de la información y la gestión de incidentes.

Marco normativo: tabla de referencia

Referencia	Aporte al BC/DR
NIST SP 800-34 Rev.1	Orienta el desarrollo formal de planes de contingencia y la relación entre continuidad, resiliencia y ciclo de vida del sistema.
NIST CSF 2.0	Integra la recuperación como función esencial dentro de la gestión del riesgo cibernético.
ISO 22301	Define el marco de sistema de gestión de continuidad del negocio y la mejora continua.
ISO/IEC 27001	Relaciona la disponibilidad, integridad y confidencialidad con la gestión formal del riesgo.
MSPI / Resolución 500 de 2021	Aterriza la seguridad y privacidad de la información en entidades colombianas mediante el ciclo PHVA.
Directiva 02 de 2022	Exige planes de continuidad y ejercicios de validación frente a riesgos de seguridad de la información.
Decreto 338 de 2022	Fortalece la gobernanza y el enfoque de prevención, respuesta, recuperación y aprendizaje.

7. Gobierno del BC/DR y responsabilidades

La continuidad del negocio no debe recaer exclusivamente en el equipo técnico de backup. Un plan efectivo requiere patrocinio de la alta dirección, validación de prioridades por parte de los dueños de proceso, coordinación de seguridad de la información, operación técnica por el área de infraestructura y mecanismos de seguimiento por control interno o auditoría. Esta distribución es coherente con el enfoque de sistema de gestión y con la necesidad de que las decisiones sobre RTO, RPO y niveles de servicio se adopten en función del impacto al negocio y no solo del criterio técnico.

En términos prácticos, la alta dirección debe aprobar la política de continuidad y asignar recursos; el líder de tecnología o infraestructura debe administrar la plataforma Veeam, los repositorios, las ejecuciones de jobs, el monitoreo y las restauraciones; seguridad de la información debe revisar el hardening, la segregación, los accesos privilegiados, la protección contra ransomware y la alineación normativa; los dueños de proceso deben priorizar servicios y validar el impacto de la indisponibilidad; y auditoría o control interno debe verificar evidencia de cumplimiento, efectividad de las pruebas y tratamiento de hallazgos.

Gobierno del BC/DR: matriz de roles

Rol	Responsabilidad principal	Evidencia esperada
Alta dirección	Aprobación del plan, asignación de recursos y priorización estratégica.	Acta o aprobación formal del documento y del presupuesto asociado.
Líder TI / Infraestructura	Administración de Veeam, repositorios, restauraciones y operación de jobs.	Consola de administración, procedimientos operativos y bitácoras de respaldo.
Seguridad de la información	Revisión de hardening, accesos, cifrado, inmutabilidad y riesgo residual.	Matrices de control, informes de revisión y planes de tratamiento.
Dueños de proceso	Definición de criticidad, RTO, RPO y validación de restauraciones funcionales.	Matriz de criticidad y actas de aceptación de pruebas.
Control interno / Auditoría	Seguimiento a indicadores, evidencia, hallazgos y mejora continua.	Informes de auditoría y planes de acción.

8. Estrategia institucional de backup y recuperación

8.1 Principios de diseño

La estrategia institucional propuesta adopta como principio rector el esquema 3-2-1-1-0, el cual en la guía oficial de mejores prácticas de Veeam se resume así: tres copias de los datos, en dos medios diferentes, una copia fuera del sitio, una copia offline, air-gapped o inmutable, y cero errores en la verificación de recuperación [Ref. R9, R10]. Este principio permite pasar de una visión centrada en "tener backups" a una visión centrada en "garantizar recuperabilidad".

Bajo este principio, el appliance de 200 TB debe considerarse como un componente esencial, pero no como la única barrera. Si todas las copias residen en la misma ubicación física, bajo la misma zona de confianza o sujetas al mismo conjunto de credenciales administrativas, la organización mantiene una superficie de riesgo alta frente a fallas locales, sabotaje, cifrado masivo, borrado no autorizado o desastre físico. Por ello, el plan recomienda complementar el almacenamiento actual con una copia secundaria fuera del sitio y, cuando la arquitectura lo permita, con un repositorio endurecido o con inmutabilidad.

8.2 Clasificación de activos y definición de RTO/RPO

Ningún esquema BC/DR es eficiente si trata todos los servicios con la misma criticidad. El primer paso operativo debe ser clasificar activos y servicios en niveles de impacto. Los servicios críticos —por ejemplo, bases de datos transaccionales, sistemas misionales, autenticación corporativa, servicios de virtualización y repositorios documentales esenciales— deben tener respaldos más frecuentes y prioridades de restauración superiores. Los servicios de soporte, históricos o no productivos pueden manejar ventanas más amplias, siempre que el riesgo haya sido formalmente aceptado.

El RTO representa el tiempo máximo tolerable para restablecer un servicio luego de una interrupción; el RPO representa la máxima pérdida de datos aceptable medida en tiempo. Estos indicadores deben definirse con participación del negocio, porque inciden directamente en el diseño de frecuencias de backup, en el costo de almacenamiento, en las capacidades de replicación y en la forma de probar la recuperación. Un RPO de pocas horas o minutos exige una estrategia más exigente que un RPO diario; del mismo modo, un RTO de una hora no se soporta con el mismo procedimiento que un RTO de un día.

Clase	Descripción	RTO de referencia	RPO de referencia
Crítica	Servicios cuya caída detiene la operación misional o compromete obligaciones regulatorias.	1 a 4 horas	15 min a 4 horas
Alta	Servicios relevantes para operación institucional, con afectación importante pero controlable.	4 a 8 horas	4 a 8 horas
Media	Servicios de soporte o administrativos con alternativas temporales de contingencia.	8 a 24 horas	8 a 24 horas
Baja	Servicios históricos, no productivos o de baja dependencia operativa.	24 a 72 horas	24 a 48 horas

8.3 Esquema de copias recomendado

Sobre la base tecnológica existente, el esquema recomendado consiste en mantener respaldos primarios hacia el appliance de 200 TB, con políticas diferenciadas por criticidad, y complementar ese almacenamiento con un segundo destino de copia para cumplimiento del principio off-site. El segundo destino puede materializarse mediante repositorio remoto, almacenamiento en la nube, cinta u otro medio técnicamente viable para la organización. Si la segunda copia no se encuentra todavía implementada, debe registrarse como brecha de continuidad y tratarse con prioridad alta.

Para servicios críticos, se recomienda usar backups incrementales diarios y puntos de restauración consistentes con el RPO definido, acompañados por una política de retención de largo plazo. La documentación oficial de Veeam indica que la política de retención GFS (Grandfather-Father-Son) permite conservar respaldos por semanas, meses y años mediante full backups sintéticos o activos marcados con banderas semanales, mensuales o anuales [Ref. R19]. Esto es especialmente útil para obligaciones de trazabilidad, conservación y recuperación histórica.

Cuando el destino sea un appliance deduplicante, Veeam recomienda considerar el método de active full para backup copy con GFS, dado que puede mejorar el rendimiento y reducir la carga sobre el repositorio de destino [Ref. R20]. Esta recomendación debe evaluarse en función del fabricante del appliance, del comportamiento del dedupe, de la ventana de respaldo disponible y del impacto de la cifración sobre la deduplicación.

Tabla de esquema de copias por tipo de activo

Tipo de activo	Frecuencia sugerida	Retención corta	Retención larga	Observación
Bases de datos críticas	Incremental diario / según RPO	30 a 60 días	GFS mensual y anual	Requiere pruebas frecuentes de restauración transaccional.
Máquinas virtuales críticas	Diaria	30 días	GFS semanal y mensual	Validar arranque y servicios dependientes.
Servidores de infraestructura	Diaria	21 a 30 días	GFS mensual	Incluye AD, DNS, DHCP y otros servicios base.
Repositorios documentales	Diaria o cada cambio relevante	30 a 90 días	GFS mensual y anual	Atender sensibilidad de datos y obligaciones de conservación.
No productivos / pruebas	Semanal o según necesidad	14 a 30 días	Opcional	No deben competir con servicios críticos por la ventana de backup.

9. Configuración recomendada para Veeam Backup y appliance de 200 TB

9.1 Seguridad del entorno de backup

La plataforma de respaldo debe tratarse como infraestructura crítica. No es recomendable administrarla con las mismas credenciales o desde las mismas zonas de red que la producción general. El entorno de backup debe tener administración separada, cuentas con privilegio mínimo, autenticación reforzada, segmentación de red y monitoreo específico. En la documentación oficial, el Security & Compliance Analyzer de Veeam verifica parámetros de configuración del sistema operativo y del producto, incluyendo aspectos de seguridad de la infraestructura [Ref. R21].

En consecuencia, la organización debe revisar y documentar, como mínimo, los siguientes controles: separación de cuentas administrativas; restricción de acceso al servidor de backup y al appliance; control de cambios; actualización y parcheo; registro de eventos; acceso por redes administrativas segregadas; resguardo de credenciales; y custodia segura de las llaves o contraseñas de cifrado. El acceso de terceros o de personal no autorizado al entorno BC/DR debe estar formalmente aprobado y trazado.

Mantener el servidor de backup y el appliance fuera del dominio de uso común cuando la arquitectura y el riesgo lo justifiquen, o al menos fuertemente segregados del entorno de usuario final.

Restringir las conexiones de administración al mínimo indispensable y registrar cualquier acceso privilegiado.

Definir procedimientos formales de backup de configuración, custodia de contraseñas de cifrado y recuperación del propio servidor de backup.

Asegurar sincronización de hora, actualización del sistema operativo, revisión de antivirus o controles equivalentes y análisis de postura de seguridad.

9.2 Cifrado y protección de los respaldos

El cifrado de las copias de seguridad es una práctica obligatoria cuando los respaldos contienen información sensible, personal, contractual, financiera o estratégica. La documentación de Veeam indica que el producto utiliza claves específicas de cifrado de datos para proteger los archivos de backup, y que estas claves se resguardan cifradas mediante una contraseña o una clave de KMS según el escenario [Ref. R22]. Asimismo, el cifrado puede habilitarse en los jobs de backup, transmitiendo los datos cifrados hacia el repositorio de destino [Ref. R23].

- ① No obstante, el cifrado debe implementarse con gobierno. El plan debe definir quién administra las contraseñas o llaves, cómo se resguardan, quién tiene autorización para usarlas y cómo se recuperan en un escenario de desastre. Una mala gestión de las claves puede convertir un respaldo válido en un respaldo irrecuperable. Además, debe considerarse que la cifración puede afectar la deduplicación en ciertos tipos de almacenamiento, por lo que cualquier decisión debe analizar el equilibrio entre seguridad, desempeño y capacidad.

9.3 Inmutabilidad y repositorio endurecido

La documentación oficial de Veeam señala que un Hardened Repository basado en Linux puede utilizarse para proteger los archivos de backup frente a pérdida causada por actividad maliciosa o acciones no planificadas [Ref. R24]. Desde el enfoque BC/DR, esto es fundamental: si un atacante compromete el entorno productivo y luego altera o elimina los respaldos, la organización puede perder simultáneamente la operación y la posibilidad de recuperarse. Por eso, la inmutabilidad no debe verse como una mejora opcional sino como un control de resiliencia de alto valor.

En el contexto del appliance de 200 TB, debe evaluarse si el fabricante o la arquitectura actual permiten cumplir objetivos de inmutabilidad, WORM, snapshots protegidos o mecanismos equivalentes. Si la plataforma local no lo soporta de forma suficiente, se debe complementar con una segunda copia en repositorio endurecido o almacenamiento que provea garantías equivalentes. Lo importante no es el nombre del producto, sino la capacidad objetiva de impedir la eliminación o modificación no autorizada durante la ventana de retención definida.

9.4 Detección de malware y restauración segura

Las versiones recientes de la documentación de Veeam describen capacidades de detección de malware, escaneo de backups y secure restore, mediante motores propios o de terceros, así como mediante reglas YARA y análisis de actividad sospechosa [Ref. R25]. Estas funcionalidades pueden aportar información crítica para decidir desde qué restore point conviene recuperar un sistema después de un incidente de ransomware o de una sospecha de compromiso. La recuperación segura debe formar parte del plan y no improvisarse en medio de la crisis.

Por lo anterior, la organización debe definir el tratamiento de puntos de restauración sospechosos, los criterios para marcar una máquina o backup como limpio, y la secuencia de análisis previo a poner nuevamente en operación un servicio restaurado. Restaurar rápido no es suficiente; restaurar datos comprometidos o reinfectados puede agravar el incidente. La premisa del BC/DR debe ser recuperar con rapidez, pero también con confianza razonable en la integridad del punto restaurado.

10. Verificación de integridad, pruebas y simulacros

10.1 Verificación de integridad

La integridad de las copias no puede asumirse; debe demostrarse. Veeam permite ejecutar periódicamente un Health Check sobre el último restore point de una cadena de backup. Durante esta verificación, el producto realiza una comprobación CRC de los metadatos y una verificación por hash de los bloques de datos de la máquina virtual dentro del archivo de backup para confirmar su integridad [Ref. R26]. Si se detecta corrupción, la cadena o los restore points afectados pueden ser marcados como corruptos y debe iniciarse la remediación correspondiente.

A nivel institucional, el plan debe establecer que los health checks se programen con mayor prioridad en los servicios críticos, que sus resultados se registren y que toda inconsistencia sea tratada como un hallazgo relevante de continuidad. Un backup corrupto, un punto inconsistente o una cadena incompleta no deben permanecer en silencio dentro del repositorio. El responsable de operación debe generar acción correctiva, documentar causa raíz cuando sea posible y validar la generación de un nuevo punto confiable.

10.2 Pruebas de recuperación

La verificación de integridad es necesaria, pero no suficiente. El BC/DR exige pruebas reales de restauración. Veeam describe en su tecnología SureBackup la posibilidad de verificar respaldos y ejecutar análisis de contenido para detectar rastros de malware o datos no deseados, incluso sin laboratorio virtual en ciertos escenarios [Ref. R27]. En términos de gestión, esto debe traducirse en un programa regular de pruebas que combine restauraciones de archivos, restauraciones de servidores, pruebas funcionales de aplicaciones y simulacros integrales de recuperación.

Se recomienda manejar tres niveles de prueba: pruebas técnicas frecuentes sobre archivos y máquinas puntuales; pruebas funcionales mensuales o bimestrales de servicios relevantes; y simulacros integrales trimestrales o semestrales para los servicios más críticos. Adicionalmente, debe realizarse por lo menos un ejercicio anual de recuperación mayor que permita medir tiempos reales, interdependencias, procedimientos de escalamiento, canales de comunicación y capacidad del equipo para operar en contingencia. La Directiva 02 de 2022 refuerza precisamente la obligación de realizar ejercicios que prueben la efectividad del plan [Ref. R12].

Tipo de prueba	Objetivo	Frecuencia sugerida	Evidencia
Restauración de archivo	Validar acceso a archivos individuales y tiempos básicos de recuperación.	Mensual	Bitácora de restauración y validación del usuario responsable.
Restauración de VM/servidor	Comprobar recuperabilidad del sistema y consistencia del arranque.	Mensual o bimestral	Capturas, logs del job y acta de validación.
Prueba funcional de aplicación	Confirmar que el servicio restaurado opera correctamente desde el punto de vista del proceso.	Trimestral	Prueba funcional firmada por dueño del proceso.
Simulacro de desastre	Medir tiempos, coordinación y secuencia integral de recuperación.	Semestral o anual	Informe de ejercicio, hallazgos y plan de mejora.

10.3 Criterios mínimos de aceptación

El backup probado debe abrirse, montarse o restaurarse sin errores críticos.

Los tiempos de restauración deben medirse y compararse con el RTO aprobado para el servicio.

Los datos restaurados deben corresponder al RPO esperado y no evidenciar corrupción o pérdida superior a la tolerada.

Las dependencias del servicio restaurado deben validarse; no basta con recuperar el servidor si la aplicación no opera.

Toda desviación debe generar acción correctiva, ajuste del procedimiento o revisión del diseño del backup.

11.Activación del plan y recuperación operativa

El plan BC/DR debe activarse cuando un evento comprometa o amenace de manera grave la continuidad de uno o más servicios críticos. Entre los disparadores típicos se encuentran: indisponibilidad prolongada de plataforma, corrupción masiva de datos, falla del almacenamiento primario, imposibilidad de operar el servicio en la sede principal, cifrado de información por ransomware, borrado no autorizado de activos, compromiso del entorno virtual o afectación severa del propio repositorio de backup. La activación no debe depender del criterio improvisado de una sola persona; debe sustentarse en umbrales y responsables previamente definidos.

Una vez declarado el evento, se debe ejecutar un flujo ordenado que contemple: confirmación del incidente, análisis preliminar del impacto, contención o aislamiento según corresponda, verificación del estado del entorno de backup, selección del restore point más seguro y más cercano al RPO aprobado, restauración técnica, validación funcional y autorización de retorno a operación. Este proceso debe quedar respaldado por bitácoras, responsables, tiempos registrados y lecciones aprendidas. El enfoque de recuperación y aprendizaje también es coherente con el Decreto 338 de 2022 [Ref. R13].

Secuencia recomendada de activación del BC/DR



Este flujo ordenado garantiza que la recuperación se ejecute de forma controlada, trazable y alineada con los objetivos de RTO y RPO definidos para cada servicio crítico.

12. Indicadores, seguimiento y mejora continua

Para que el BC/DR sea gestionable, debe contar con métricas periódicas. No basta con afirmar que los jobs ejecutan; se requiere medir calidad, cobertura y recuperabilidad. Entre los indicadores mínimos recomendados se encuentran: porcentaje de jobs exitosos, número de fallas por período, porcentaje de activos críticos protegidos, consumo y crecimiento del appliance, cumplimiento de ventanas de respaldo, número de health checks exitosos, porcentaje de restauraciones probadas, tiempo promedio real de restauración y porcentaje de pruebas que cumplen RTO/RPO.

La mejora continua implica revisar estos indicadores, compararlos con los objetivos aprobados, priorizar hallazgos y actualizar el plan. El MSPI estructura su implementación sobre el ciclo PHVA y exige, en su documento maestro, fases de diagnóstico, planificación, operación, evaluación de desempeño y mejoramiento continuo [Ref. R8]. En consecuencia, el plan BC/DR debe revisarse por lo menos una vez al año y cada vez que existan cambios de arquitectura, nuevos sistemas críticos, incidentes reales, variaciones de licenciamiento, crecimiento relevante de datos o nuevos riesgos identificados.

Tabla de indicadores clave de desempeño

Indicador	Meta sugerida	Frecuencia de revisión
Jobs exitosos	≥ 98 %	Diaria / semanal
Activos críticos cubiertos por backup	100 %	Mensual
Health checks satisfactorios	≥ 95 %	Mensual
Pruebas de restauración ejecutadas según plan	100 % del calendario	Mensual / trimestral
Cumplimiento de RTO en pruebas	≥ 90 %	Trimestral
Crecimiento controlado del repositorio	Según capacidad y planeación	Mensual

13. Conclusiones

El presente documento demuestra que un Plan BC/DR efectivo requiere mucho más que la existencia de un software de backup y de un repositorio amplio. La combinación de Veeam Backup con un appliance de 200 TB es una base sólida, pero solo alcanza madurez real cuando se integra con gobierno, clasificación por criticidad, diseño de retención, cifrado, control de acceso, inmutabilidad o aislamiento, verificación de integridad, pruebas periódicas y mecanismos formales de activación y recuperación. Esa es la diferencia entre almacenar copias y garantizar continuidad.

El marco normativo revisado confirma que la continuidad, la seguridad de la información y la recuperación verificable no son opcionales. NIST, ISO, CISA y el marco colombiano coinciden en exigir preparación documentada, controles proporcionales al riesgo, pruebas de efectividad y mejora continua [Ref. R1, R2, R3, R5, R7, R12]. Por ello, la organización debe tratar este plan como un instrumento vivo: sujeto a seguimiento, ejercicios, ajuste técnico y actualización documental, no como un simple anexo de cumplimiento.

Implementado correctamente, este plan permitirá reducir la probabilidad de pérdida irreversible de información, mejorar la respuesta frente a incidentes, acortar los tiempos de recuperación, proteger la confianza institucional y fortalecer la capacidad de resiliencia ante ransomware, fallas de infraestructura y eventos disruptivos. En otras palabras, permitirá que el entorno actual de Veeam y el appliance de 200 TB evolucionen desde una plataforma de almacenamiento hacia una verdadera capacidad institucional de recuperación.

14. Recomendaciones finales

Matriz de criticidad

Formalizar y aprobar la matriz de criticidad de servicios, con RTO y RPO validados por los dueños de proceso.

Cifrado y custodia

Habilitar cifrado en jobs y copias de configuración, con custodia formal de contraseñas o claves.

Calendario de pruebas

Establecer un calendario de pruebas mensuales, trimestrales y anuales, con evidencia y acciones de mejora.

Secuencia de activación

Documentar y ensayar la secuencia completa de activación del BC/DR ante eventos de ransomware o indisponibilidad mayor.

Principio 3-2-1-1-0

Mantener el appliance de 200 TB como repositorio principal, pero implementar o planificar una segunda copia off-site y una copia inmutable u offline para alinearse con 3-2-1-1-0.

Health Check periódico

Programar Health Check periódico y registrar el tratamiento de cualquier corrupción detectada.

Hardening del entorno

Revisar el hardening del entorno de respaldo mediante Security & Compliance Analyzer y controles internos de seguridad.

15. Referencias

R1. NIST. SP 800–34 Rev.1 – Contingency Planning Guide for Federal Information Systems. Disponible en:

<https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final>

R2. NIST. Cybersecurity Framework (CSF) 2.0. Disponible en: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

R3. CISA. StopRansomware Guide. Disponible en: <https://www.cisa.gov/stopransomware/ransomware-guide>

R4. NIST. Recover Function – Cybersecurity Framework. Disponible en: <https://www.nist.gov/cyberframework/recover>

R5. ISO. ISO 22301:2019 – Business continuity management systems. Disponible en:

<https://www.iso.org/es/contents/data/standard/07/51/75106.html>

R6. ISO. ISO/IEC 27001:2022 – Information security management systems. Disponible en:

<https://www.iso.org/es/norma/27001>

R7. MinTIC. MSPI – portal de Seguridad y Privacidad de la Información. Disponible en:

<https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>

R8. MinTIC. Modelo de Seguridad y Privacidad de la Información – Documento Maestro. Disponible en:

https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

R9. Veeam. Veeam Backup & Replication Best Practice Guide – Infrastructure Overview. Disponible en:

https://bp.veeam.com/vbr/1_Assessment/A_Infra_Overview/infra_overview.html

R10. Veeam. Protect – Veeam Backup & Replication Security Best Practice Guide. Disponible en:

<https://bp.veeam.com/security/Design-and-implementation/Protect.html>

R11. MinTIC. Resolución 500 de 2021. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

R12. Función Pública / Presidencia. Directiva Presidencial 02 de 2022. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=179306>

R13. Función Pública. Decreto 338 de 2022. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>

R14. Función Pública. Ley 1581 de 2012. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

R15. Secretaría del Senado. Ley 1273 de 2009. Disponible en: https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

R16. ISO. ISO/TS 22317:2021 – Guidelines for business impact analysis. Disponible en: <https://www.iso.org/standard/79000.html>

R17. Función Pública. Ley 1712 de 2014. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

R18. Función Pública. Decreto 1078 de 2015. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888>

R19. Veeam. Long-Term Retention Policy (GFS). Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/backup_copy_gfs.html

R20. Veeam. Backup Copy GFS Methods. Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/backup_copy_gfs_modes.html

R21. Veeam. Security & Compliance Analyzer. Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/best_practices_analyzer.html

R22. Veeam. How Backup Data Encryption Works. Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/encryption_hiw.html

R23. Veeam. Encrypting Backup Jobs. Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/encrypting_backup_jobs.html

R24. Veeam. Hardened Repository. Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/hardened_repository.html

R25. Veeam. Malware Detection. Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/malware_detection.html

R26. Veeam. Health Check for Backup Files. Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/backup_health_check.html

R27. Veeam. How SureBackup Works. Disponible en: https://helpcenter.veeam.com/docs/vbr/userguide/surebackup_hiw.html

Cierre del documento

Tipo de documento

Plan institucional de continuidad del negocio y recuperación ante desastres

Base tecnológica

Veeam Backup con almacenamiento de copias en appliance de 200 TB

Fecha de emisión

18 de marzo de 2026



Propósito del documento: establecer los lineamientos de gobierno, protección, respaldo, verificación, recuperación y mejora continua para asegurar la disponibilidad e integridad de la información y de los servicios críticos frente a incidentes operativos, fallas de infraestructura y eventos de ciberseguridad.

Documento elaborado con enfoque de continuidad, resiliencia operativa, seguridad de la información y buenas prácticas de recuperación verificable.

Este documento debe tratarse como un instrumento vivo: sujeto a seguimiento, ejercicios, ajuste técnico y actualización documental. Revisión mínima anual o ante cambios de arquitectura, nuevos sistemas críticos, incidentes reales, variaciones de licenciamiento, crecimiento relevante de datos o nuevos riesgos identificados.