Respaldo y recuperación ante desastres

Políticas y despacho de respaldos, repositorio inmutable compatible con S3, verificación de cada respaldo por restauración aislada, PITR multi-motor, planes DR semi-automáticos y federación entre sitios.

Modelo general

Estado: Disponible

El módulo de respaldos reside en el agente instalado en cada servidor. La consola programa las políticas, despacha los trabajos y muestra los resultados; las credenciales de las bases de datos las resuelve el agente en el propio servidor y nunca pasan por la consola. El alcance de cada agente es su propio host: protege únicamente el servidor donde reside y todo lo que ese servidor contiene.

Cada respaldo:

- Viaja en flujo, sin archivos temporales intermedios, cifrado con **AES-256-GCM**.
- Se acompaña de un manifiesto con el motor y su versión, los tiempos de inicio y fin, los tamaños, la huella SHA-256 del artefacto, el conteo de filas por tabla y, tras su verificación, el tiempo de restauración medido.
- Se rige por una política de retención por generaciones: diaria, semanal, mensual y anual.

Destinos y repositorio inmutable

Estado: Disponible

Estado por destino:

- **Disponible:** el repositorio de objetos S3 — la capa S3 la aporta siempre **MinIO**, desplegado por el proveedor —, incluido el **almacenamiento NAS**, que se sirve sobre S3 y ya opera así en producción, y el almacenamiento de otro sitio federado.
- **Compromiso (hoja de ruta comprometida): HPE 3PAR**, servido igualmente sobre S3 (capa MinIO).
- **Hoja de ruta:** la cinta y los demás tipos de destino.

Los destinos disponibles son intercambiables entre sí.

- **Repositorio de objetos compatible con S3 con bloqueo de objetos inmutable.** Al punto sellado se le aplica una retención que impide su borrado durante su periodo, en el modo de cumplimiento cuando la política protege puntos críticos. El patrón de uso exige un contenedor dedicado por agente u organización, con credenciales de mínimo privilegio propias de ese agente y sin permisos de administración ni de anulación de la retención.

- **Cifrado por agente.** Cada respaldo se cifra por agente antes de salir hacia su destino; comprometer un destino no expone respaldos en claro.
- **Segunda copia.** La política puede definir un segundo destino, inmediato o programado. La copia verifica la huella durante la transferencia: si no coincide, la copia se aborta y el parcial se descarta.
- **Copia desconectada (hoja de ruta).** Un medio local desconectable aporta la copia aislada frente a programas de secuestro de datos.

Verificación de cada respaldo

Estado: Disponible

Un respaldo que nunca se restaura es una promesa, no un respaldo. Por eso **cada respaldo se verifica mediante una restauración en un entorno aislado (sandbox)**, sin red hacia producción, siguiendo este orden:

1. Análisis antivirus del contenido descifrado. Si el análisis no está disponible en ese servidor, el informe lo declara como omitido, sin fingir que se realizó.
2. Arranque del entorno aislado y espera a que el motor responda sano.
3. Restauración del artefacto y conteo de filas por tabla, que debe coincidir exactamente con el manifiesto.
4. Medición del tiempo de restauración, que queda registrado en el manifiesto.
5. En la verificación extendida, pruebas a los portales declarados y captura real de la comprobación.
6. Destrucción del entorno aislado en todos los casos.

La verificación produce un **informe** que acompaña al respaldo. Un respaldo marcado como comprometido se marca y se aísla, y nunca se borra automáticamente; restaurar un punto marcado exige una aprobación explícita y registrada del riesgo.

Además de la restauración, un chequeo periódico de integridad vuelve a leer y a calcular la huella de cada artefacto y la contrasta con su manifiesto, para detectar corrupción silenciosa.

Motores y recuperación a un punto en el tiempo (PITR)

Estado: Disponible

Motor	Respaldo completo	Incremental	Recuperación a un instante
PostgreSQL	Volcado en formato personalizado	Copia base con segmentos de registro de transacciones archivados	Restauración de la base y reproducción del registro hasta la fecha y hora o la posición pedidas
MySQL y MariaDB	Volcado transaccional	Segmentos del registro binario desde la posición capturada en la base	Restauración de la base y reproducción del registro hasta la fecha y hora o la posición pedidas
SQL Server	Copia completa de la base	Copias del registro de transacciones	

Motor	Respaldo completo	Incremental	Recuperación a un instante
			Restauración sin recuperar, aplicación de los registros hasta el instante pedido y cierre con recuperación
SQLite	Copia completa, siempre	No aplica	Al último respaldo

La recuperación a un punto en el tiempo está **verificada de extremo a extremo en los tres motores con registros transaccionales**: PostgreSQL, MariaDB y SQL Server. Antes de tocar producción, la restauración se ejecuta primero en el entorno aislado y puede comprobarse con una consulta de solo lectura sobre el instante elegido.

La poda por retención nunca deja una cadena rota: si se conserva un incremental, se conservan su base y todos los incrementales intermedios.

También se respaldan volúmenes y rutas de archivos, con índice por archivo que permite restaurar un solo archivo sin restaurar el volumen completo, así como máquinas virtuales y contenedores de hipervisor en Proxmox VE, y la propia consola.

Respaldo continuo

Estado: Disponible, para cargas cuyo objetivo de pérdida de datos sea de minutos.

El respaldo continuo envía los segmentos de registro a medida que se cierran, en orden, verifica cada subida volviendo a leer el objeto y comparando su huella, y solo entonces confirma la posición. Su medida operativa es el retraso entre el momento actual y el último segmento confirmado, que representa la pérdida potencial real y debe vigilarse y alertarse. El manual de usuario declara el límite verificado de esta función, que debe consultarse antes de presentarla como verificada contra motores en producción.

Planes de recuperación ante desastres (DR)

Estado: Disponible

Un plan de recuperación es un plan versionado que reconstruye en orden: red, volúmenes, datos y aplicaciones, esperando a que cada capa responda sana antes de continuar.

- **Preparación automática.** La detección del fallo y la preparación del plan —punto verificado más reciente, comprobaciones de destino y orden de ejecución— son automáticas.
- **Ejecución con aprobación humana.** La ejecución es **semi-automática**: requiere la aprobación de una persona identificada, distinta de quien configuró el plan, por la consola o por los canales de guardia previstos. Si nadie autoriza, no se ejecuta nada que afecte a datos.
- **Simulacros.** Los planes se ejercitan con simulacros periódicos que restauran de verdad en un entorno aislado y miden los tiempos contra los objetivos del nivel contratado, con informe firmado.

- **Federación entre sitios.** Los destinos de respaldo pueden ser otro sitio de la federación, y un plan puede reconstruir en el sitio alterno desde ese respaldo federado. Cada sitio sigue operando de forma autónoma si la federación no está disponible.

Objetivos de tiempo y de punto de recuperación

Las fuentes públicas del expediente fijan los objetivos **de diseño por nivel** siguientes, y declaran expresamente que no se promete pérdida cero: el diseño se basa en instantáneas frecuentes y en el respaldo continuo, no en replicación síncrona.

Nivel	Objetivo de punto de recuperación (RPO)	Objetivo de tiempo de recuperación (RTO)
Comercial Esencial	24 horas	4 horas
Comercial Profesional	1 hora	1 hora
Gobierno	Contractual; diseño: 15 minutos	Contractual; diseño: 30 minutos

El tiempo que vale frente a un auditor es el **medido** en cada verificación y en cada simulacro, que queda registrado en el manifiesto y en el informe correspondiente.

Cinta

Estado: Hoja de ruta comprometida. La cinta forma parte del programa de destinos comprometido (octubre de 2026); esta sección recoge su diseño objetivo, con la limitación declarada en el manual de usuario.

El respaldo a cinta con controlador genérico y la infraestructura completa de cinta sobre esa base — conjuntos de medios por generaciones, custodia de medios fuera del sitio con registro de movimientos, varios flujos en paralelo y conjuntos con retención absoluta— forman parte del producto. La validación contra una librería física concreta queda sujeta a la matriz de compatibilidad del sitio; la validación realizada consta contra librería virtual.