



Recuperación ante desastres

Percus SpA · octubre de 2026

Versión web: <https://docs.percus.video/es/security/disaster-recovery>

© Percus SpA

Esta página describe cómo Percus recupera su plataforma ante fallas y pérdida de datos: qué escenarios están cubiertos, cómo se resuelve cada uno, cuánto tarda la recuperación y qué se ha probado realmente. Refleja el estado a **octubre de 2026**, incluido lo que todavía no está cubierto.

Percus mantiene además un runbook operativo interno con el procedimiento paso a paso de cada escenario. No se publica porque contiene detalles de la infraestructura.

Alcance

- **Servicio de visualización:** la configuración del video y la entrega del reproductor que usa el navegador del destinatario para cargar y reproducir un video personalizado.
- **Backoffice:** la aplicación web y las APIs con las que los clientes de Percus gestionan proyectos, plantillas, canales de distribución y usuarios.
- **Datos:** la base de datos relacional (organizaciones, usuarios, proyectos, plantillas, canales), los datos de personalización por destinatario, los recursos de las plantillas y la analítica.

Objetivos de recuperación

	Compromiso contractual	Objetivo interno	Medido
RTO — tiempo para restablecer el servicio	4 horas	30 minutos para una restauración de la base de datos	Failover de la base: ~15–17 s. Restauración de la base desde un snapshot: ~12 min hasta quedar lista (ver Pruebas)
RPO — máxima pérdida de datos	30 días (ventana de retención de backups)	~5 minutos (granularidad de la recuperación a un punto en el tiempo)	—

Los valores contractuales son los publicados en [Niveles de servicio](#). Los objetivos internos son la meta hacia la que trabaja Percus; **son metas, no compromisos**. El objetivo de 30 minutos es lo que debe durar como máximo un evento de recuperación para que la plataforma sostenga una disponibilidad mensual de 99,9%.

Cómo está construida la plataforma para recuperarse

- **Una región de AWS, dos zonas de disponibilidad.** Producción opera en AWS `us-east-1`. El cómputo es serverless y AWS lo distribuye entre zonas de disponibilidad; la red tiene un NAT gateway por zona de disponibilidad.
- **Base de datos relacional con réplica en espera.** Un writer y un reader en espera en dos zonas de disponibilidad, con failover automático. Cifrada en reposo con una llave administrada por Percus.
- **Backups continuos.** La base de datos relacional mantiene recuperación a un punto en el tiempo por 30 días. Los datos de personalización por destinatario la mantienen por 35 días.
- **Almacenamiento de archivos versionado.** El almacenamiento de plantillas y recursos conserva las versiones anteriores de cada archivo, de modo que un archivo borrado o sobrescrito se puede recuperar.

- **Infraestructura como código.** La infraestructura está definida en código y se despliega con pipelines automatizados, así que los componentes se pueden reconstruir desde el control de versiones. Algunas configuraciones (las zonas DNS, y la conexión al repositorio y los secretos del hosting del backoffice) se configuran manualmente.
- **Credenciales, llaves y datos protegidos.** Las credenciales de la base de datos, las llaves de cifrado y los secretos de los que dependen los datos almacenados se conservan aunque se elimine la infraestructura que los creó. La base de datos relacional tiene protección contra borrado; la tabla de datos por destinatario y su llave también se conservan aunque se elimine esa infraestructura.

Historial de backups

El cluster de base de datos actual reemplazó al anterior el 6 de octubre de 2026 (UTC). Su historial de recuperación a un punto en el tiempo empieza en esa fecha y alcanza la ventana completa de 30 días el 5 de noviembre de 2026.

Escenarios

Escenario	Recuperación	Tiempo esperado	Estado
Falla una instancia de la base de datos o una zona de disponibilidad	Failover automático a la réplica en espera de la otra zona. No se pierden datos	Segundos	Probado (octubre de 2026)
Datos relacionales borrados o dañados por error (una operación, una versión defectuosa, corrupción)	Restauración a un punto en el tiempo justo anterior al problema en una base nueva, cambio de la plataforma a esa base y verificación	Objetivo 30 min	Restauración medida ; procedimiento de cambio en validación
Se pierde el cluster de base de datos completo	Restauración al último punto en el tiempo disponible en un cluster nuevo y cambio de la plataforma a ese cluster	Objetivo 30 min	Restauración medida ; procedimiento de cambio en validación
Se pierden o dañan los datos de personalización por destinatario	Restauración a un punto en el tiempo de esos datos en una tabla nueva, o el cliente vuelve a cargar su archivo de datos	A definir en el ensayo	Documentado, ensayo pendiente
Se borra o sobrescribe un archivo de plantilla o un recurso	Restauración de la versión anterior desde el almacenamiento versionado	Minutos	Documentado
Se pierde o se rompe la entrega del reproductor o del SDK de incrustación	Nuevo despliegue desde el control de versiones	Minutos	Documentado
Una versión nueva rompe la plataforma	Nuevo despliegue de la versión anterior. Redespregar no revierte los cambios de esquema de la base de datos; si la versión dañó datos, aplica el escenario de datos relacionales	Menos de una hora	Documentado ; rollback automático planificado

Escenario	Recuperación	Tiempo esperado	Estado
La región completa de AWS deja de estar disponible	Hoy no hay un procedimiento automático ni probado: la plataforma y sus backups están en una sola región	No definido	Limitación conocida

La analítica se puede recuperar desde su almacén de eventos crudos si se pierden los datos compactados; los eventos crudos que todavía no se compactaron pueden perderse. Los eventos crudos se conservan 12 meses. La analítica no afecta la entrega de videos.

Respuesta a incidentes

Detección. Alarmas de AWS CloudWatch sobre las colas de procesamiento y el envío de emails alertan al equipo de ingeniería por email. Se están implementando alertas sobre disponibilidad y errores de la API, y un monitoreo sintético externo que revisa la plataforma desde fuera de AWS como lo haría un cliente.

Roles.

Rol	Responsabilidad
Líder del incidente (CTO)	Declara el incidente, decide el camino de recuperación y aprueba el cambio de la plataforma a los datos restaurados
Operador técnico	Ejecuta el procedimiento de recuperación del runbook interno y verifica el resultado
Comunicación con clientes (Customer Success)	Mantiene informados a los clientes afectados hasta el cierre del incidente

Comunicación. Se informa a los clientes afectados a través de su contacto habitual en Percus. Para incidentes que afectan datos personales aplican los compromisos de notificación del [Anexo de protección de datos](#), incluida la notificación dentro de 24 horas.

Después del incidente. Todo incidente que requiere un procedimiento de recuperación se revisa, y el runbook y esta página se actualizan con lo aprendido.

Pruebas

La recuperación se prueba con ensayos en el ambiente de staging, que tiene la misma topología que producción (un writer y una réplica en espera en dos zonas de disponibilidad).

Fecha	Prueba	Resultado
5 y 6 de octubre de 2026	Restauración de la base desde un snapshot a un cluster nuevo, durante el cambio planificado a la base cifrada (staging y producción)	Base lista en ~13 min (staging) y ~12 min (producción)
6 de octubre de 2026	Failover forzado de la base a la otra zona de disponibilidad, y de vuelta (staging)	Promoción en ~17 s y ~15 s; la API respondió con degradación durante ~7–9 s

Fecha	Prueba	Resultado
Planificado	Ensayo completo de recuperación: restauración a un punto en el tiempo, cambio de la plataforma y verificación, cronometrado de punta a punta	—

Se realizará un ensayo completo de recuperación al menos una vez al año y después de cada cambio importante de infraestructura. Cada resultado se agrega a la tabla anterior.

Limitaciones conocidas

- **Una sola región.** No hay una recuperación probada ante la pérdida de la región completa de AWS.
- **Ensayo completo de recuperación pendiente.** La restauración está medida, pero el procedimiento completo (restauración, cambio y verificación) todavía no se cronometró de punta a punta.
- **Todavía sin rotación formal de guardia (on-call).** Se está implementando una rotación formal de guardia.
- **Detección parcial.** Las alarmas cubren el procesamiento en segundo plano y el envío de emails; las alertas sobre disponibilidad y errores de la API, y el monitoreo externo, están en curso.