DOCUMENTO OP-02 · PROGRAMA PÚBLICO V1.2

Política de respaldos, continuidad y recuperación

Directrices y objetivos de respaldo para EDUAI, Sello Tecnológico y los servicios de Innova Space Edu SpA.

Programa de continuidad publicado: identifica los controles que deben aplicarse, pero no acredita copias ya ejecutadas, cifradas o restauradas ni constituye una garantía de disponibilidad.

1. Alcance y estado

Este documento describe el programa propuesto de continuidad, respaldo y recuperación para los sistemas de Innova Space Edu SpA y sus plataformas educativas. No acredita su instalación ni constituye garantía de nivel de servicio. El repositorio público no contiene ubicaciones físicas precisas, direcciones de red, inventarios sensibles, credenciales ni claves.

---

2. Objetivo y clasificación

Separar los datos por finalidad y responsable, distinguir bases de datos de archivos binarios, registros de actividad, configuraciones imprescindibles y evidencias educativas. La institución responsable decide plazos, excepciones y condiciones de devolución de datos tratados por cuenta suya. Innova mantiene las medidas técnicas apropiadas y sus evidencias.

---

3. Almacenamiento y copias

En la etapa inicial se proyecta alojar copias cifradas de seguridad en infraestructura controlada por Innova Space Edu SpA, cuya ubicación física debe validarse; si está efectivamente en Chile, las copias quedarían alojadas allí, mientras las bases principales siguen en Supabase Free. Los respaldos incluyen exportaciones de PostgreSQL, objetos de Storage, metadatos necesarios y configuración recuperable. Los proyectos principales siguen en la región us-west-2

(Estados Unidos): almacenar una copia en Chile no traslada por sí mismo el tratamiento principal ni extingue las transferencias internacionales.

---

4. Protección de copias

El dispositivo destinado a respaldos deberá cifrarse, restringir sus permisos, proteger credenciales y claves mediante gestión separada, cifrar transmisiones, verificar firmas o checksums y registrar operaciones. No se expondrá como carpeta pública, enlace compartido o recurso accesible directamente desde Internet. La información no deberá incorporarse a repositorios de código.

---

5. Independencia y riesgo físico

Un solo dispositivo o una copia conectada permanentemente al mismo servidor no ofrece protección suficiente ante ransomware, robo, incendio o fallo simultáneo. El objetivo es disponer de al menos una segunda copia cifrada independiente, desconectada o fuera del recinto, con controles de custodia y acceso verificables. La segunda copia debe estar implementada y probada antes de declarar alta resiliencia.

---

6. Periodicidad y recuperación

Como propuesta inicial, respaldar diariamente las bases y archivos que cambian, con pruebas de integridad y alertas por fallos. La frecuencia de copias completas/incrementales, retención y capacidad se determinarán tras medir uso y crecimiento, y aprobar el RPO (pérdida máxima aceptable de datos) y RTO (tiempo objetivo de recuperación) por servicio. Sin prueba de restauración satisfactoria no se declarará cumplido ninguno de estos objetivos.

---

7. Verificación y restauración

Realizar pruebas periódicas de restauración en un entorno aislado, con datos de prueba o acceso autorizado. Comprobar tablas, políticas RLS, roles, flujos de autenticación, vínculos con archivos y lectura de objetos; registrar tiempos, integridad, incidencias, fecha de la última restauración y responsable técnico. Un respaldo que solo genera archivos pero no ha sido restaurado no se considera probado.

---

8. Retención y cierre escolar

El procedimiento de cierre a acordar con cada institución contempla aviso previo de 30 días y recordatorio 7 días antes de cada cierre anual definido por la institución; exportación autorizada; y eliminación o anonimización de datos elegibles de sistemas activos hasta 30 días después, conforme a instrucciones y excepciones legales documentadas. El plazo de respaldo y su eliminación se fijará por categoría y medio: no puede presumirse que el borrado en producción suprima automáticamente las copias.

---

9. Recuperación sin reaparición de datos eliminados

Los respaldos históricos pueden contener datos que posteriormente hayan sido suprimidos de producción. Mantener un registro mínimo, íntegro y restringido de supresiones y exclusiones, aplicarlo después de cualquier restauración y antes de reabrir accesos, y eliminar copias al vencer sus períodos aprobados. La finalidad legal no permite conservar indefinidamente toda la historia mediante copias rotativas.

---

10. Roles e incidentes

Designar al propietario de cada sistema, responsable de privacidad, administrador autorizado del respaldo y sustituto. Documentar quién puede iniciar copia, restaurar, acceder a claves y aprobar la destrucción de datos. Los incidentes de disponibilidad, pérdida, fuga o acceso indebido deberán registrarse, comunicarse al responsable del tratamiento cuando corresponda y evaluarse según el procedimiento contractual y legal.

---

11. Evidencia y vigencia

Los registros de éxito/fallo, pruebas de restauración, aprobaciones del calendario, inventario de activos y plazos reales de terceros se conservarán internamente con acceso restringido. La adopción de este programa depende de inventario, contratación, recursos, pruebas y aprobación formal. Última preparación: 11 de octubre de 2026.

Fuentes técnicas: Supabase Database Backups y eliminación de objetos de Storage. Referencia normativa: Ley 21.719.

Actualización documental y alcance por servicios — 12-10-2026

Este programa debe cubrir los servicios web administrados por Innova Space Edu SpA: EDUAI, Sello Tecnológico, aplicaciones web de clientes, servidores e intranets, documentación técnica, flujos de IA y almacenamiento que correspondan según el contrato. La inclusión de estas soluciones en el alcance no constituye declaración de que todas residan en la infraestructura propia ni de que sus copias ya hayan sido verificadas.

Los criterios por actividad se registran en RAT EDUAI y RAT Sello. Los plazos, custodios, copias fuera de línea, RPO/RTO y eliminación deben aprobarse y probarse por contrato. La coordinación interna propuesta figura en el acta de gobernanza, pendiente de ratificación y firmas.

Actualización de recuperación y retención — octubre de 2026

Los proyectos web EDUAI y Sello Tecnológico se encuentran alojados en servicios externos, mientras que el equipamiento y servidor Debian de proyectos propios solo se incorporarán a una estrategia formal de respaldo de Innova tras inventario, autorización de responsables, análisis de ubicación, evaluación de seguridad y pruebas de restauración. No se presume que una infraestructura personal sea respaldo corporativo ni que exista réplica automática.

El servicio Video Studio permanece en mantenimiento; no deben programarse reintentos de generación durante la recuperación. El historial de órdenes y movimientos E17 se custodia separado de archivos educativos, con conservación aprobada, cifrado, controles de acceso y pruebas de supresión al vencer la obligación aplicable. Los perfiles y muestras E13 requieren control reforzado de acceso y plan de borrado, aun cuando la función esté suspendida para usuarios ordinarios.
