DOCUMENTO OP-01 · GUÍA OPERATIVA PÚBLICA V1.2

Protocolos de protección de datos personales

Procedimientos públicos de referencia para Innova Space Edu SpA, EDUAI y Sello Tecnológico; sujetos a verificación operativa. Esta página muestra reglas generales; los procedimientos con credenciales, contactos de emergencia, topología y detalles explotables deberán conservarse en repositorios privados.

Directrices publicadas, sujetas a verificación. Las actividades descritas son procedimientos requeridos para cada operación; su publicación no demuestra que ya estén automatizadas o implementadas.

00. Coordinación y vigencia documental

El acta de adopción documental de 12-10-2026 propone designar a **Esthefano Gonzalo Morales Campaña** como Delegado Responsable Interno de Protección de Datos y Cumplimiento. Corresponde coordinar la revisión de RAT EDUAI y RAT Sello, las solicitudes, incidentes, proveedores, conservación y planes de auditoría. El acta pública refleja el estado de la designación; aceptación y firma societaria aún pendientes.

Los protocolos se aplican según el servicio: páginas web y hosting, servidores, intranets, integraciones, IA e investigación, EDUAI, Sello Tecnológico, seguridad y servicios físicos que requieran tratamiento. La coordinación de Innova no sustituye la condición jurídica de responsable institucional ni habilita nuevos subencargados sin evaluación y autorización.

00-A. Identidad ejecutiva y atribución de responsabilidades

La identificación pública distingue al fundador y director ejecutivo (CEO), **Esthefano Gonzalo Morales Campaña**, del administrador y representante legal informado, **Iván Eduardo Morales Sandoval**. Las funciones de coordinación operativa, administración y representación jurídica no se presumen intercambiables: su alcance debe documentarse con actos y poderes vigentes. Los desarrollos experimentales de ScientificBrain, MaleCNS y visualización científica se inventarían por separado de los tratamientos contratados con instituciones. Consultar perfil y fuentes.

La adopción de procedimientos, designación de coordinación de privacidad, firmas y evidencia de ejecución se mantienen pendientes de confirmación cuando así se indiquen en el acta de gobernanza.

---

01. Registro de actividades y responsabilidad

1. Identificar cada proceso y responsable: sitio corporativo, contacto, soporte, cuentas, proyectos, exámenes, grabaciones, mensajería, archivos, IA y publicación.
2. Registrar finalidad, base de licitud, titulares, datos, datos sensibles, receptores, país, seguridad, ubicación, conservación, eliminación y evidencia.
3. Determinar para cada contrato si Innova actúa como responsable o encargada y quién decide el tratamiento y publica contenido.
4. Actualizar el registro ante módulos nuevos, integraciones, nuevos proveedores o cambios sustanciales.

---

02. Altas de cuentas y perfiles

1. Registrar solo información imprescindible por finalidad y rol. Evitar RUT cuando no sea estrictamente necesario.
2. Validar altas y cambios de roles privilegiados; revisar que un dominio de correo no baste, por sí solo, para otorgar permisos sensibles sin controles adecuados.
3. Revisar trimestralmente usuarios privilegiados, cuentas inactivas y permisos por institución; revocar accesos al terminar la relación.
4. Probar aislamiento de datos por usuario, curso, institución y proyecto; revisar RLS y endpoints con permisos elevados.

---

03. Menores y autorizaciones

1. Identificar rango etario y fundamento legal de tratamiento; documentar autorizaciones exigibles a padres o representantes, considerando menores de 14 y datos sensibles de adolescentes menores de 16.
2. Explicar el uso de datos en lenguaje comprensible a estudiantes y representantes.
3. Separar datos académicos privados de materiales destinados a difusión pública.
4. Evaluar riesgo antes de habilitar perfiles públicos, fotografías, videos, audio, geolocalización o datos potencialmente sensibles.

03-A. Formulario familiar previo al uso de EDUAI y Sello

Preparar invitación individual a padres, madres, representantes legales o personas con cuidado personal, a través de enlace privado por correo, WhatsApp u otro canal aprobado. Confirmar la pertinencia de la autorización por edad, dato y base de licitud; menores de catorce años y datos sensibles de adolescentes menores de dieciséis años cuentan con requisitos reforzados conforme al artículo 16 quáter.

1. Vincular estudiante, institución, finalidad y versión de cuestionario sin divulgar datos de menores en el mensaje de transporte.
2. Solicitar decisión específica positiva o negativa para cada finalidad opcional, sin selección automática afirmativa; separar usos internos, exposición pública, multimedia, IA, voz y comunicaciones no necesarias.
3. Capturar declaración del adulto y firma electrónica simple, reconociendo que el enlace y nombre escrito no acreditan identidad o representación por sí solos.
4. Verificar identidad y facultad de representación mediante evidencia y responsable institucional habilitado antes de aprobar.
5. Consultar permisos vigentes desde backend antes de activar funciones; impedir usos específicos tras rechazo o revocación.
6. Permitir revocación por un canal equivalente y asegurar trazabilidad de firmas, versiones y cambios, con retención proporcional y custodia privada.
7. No incorporar botón funcional de ClaveÚnica sin habilitación legal y técnica; la integración de firma avanzada requerirá prestador acreditado.

Al 12-10-2026 los formularios, el archivo de actas y las preferencias están incorporados en código y desplegados en ambas plataformas. Persisten pruebas de representación, permisos entre roles e instituciones, seguridad de APIs, revocación, entrega de correos y evidencia de operación. La existencia de funciones no acredita su eficacia integral.

---

04. Publicación en Sello Tecnológico

1. Dejar proyectos y evidencias en modo privado/borrador por defecto hasta autorización de publicación.
2. Aplicar una revisión humana antes de publicar: consentimiento o base válida, derechos sobre contenido e imágenes, identificación de personas y minimización.
3. Bloquear publicación de RUT, notas individualizadas, antecedentes PIE/NEE, salud, teléfonos, direcciones y conversaciones privadas.
4. Disponer un mecanismo para retirar contenido, solicitar revisión de publicación y registrar quién autorizó y cuándo.
5. Auditar enlaces compartidos, buckets de Supabase Storage, URLs temporales y metadatos de medios.

---

05. IA y procesamiento de documentos en EDUAI

1. Registrar proveedor y modelo real que recibe cada solicitud; limitar por categoría de dato y actividad permitida.
2. Aplicar reducción de contexto, redacción de identificadores y análisis previo de archivos; evitar transmitir íntegramente documentos sensibles sin necesidad.

3. Verificar retención, entrenamiento, región, subencargados, términos y DPA de cada proveedor antes de habilitarlo en contexto escolar.
4. Prohibir por defecto entrenamiento externo con datos identificables de alumnos; cualquier excepción exige nueva evaluación, base de licitud y acuerdo específico.
5. Exigir revisión humana de correcciones, inferencias de perfiles y recomendaciones con impacto educativo.

05-A. Uso previsto y límites de modelos de IA de EDUAI

Los proveedores de modelos externos se incorporan para apoyar elaboración de material pedagógico, redacción, explicación y respuesta a solicitudes informativas; no para tratamiento deliberado de expedientes personales o sensibles, decisiones sobre estudiantes, perfilamiento ni entrenamiento con información identificable. Un prompt o archivo aportado por usuario puede contener accidentalmente datos protegidos, por lo que esta finalidad no equivale a garantía de aislamiento técnico.

Antes de declarar que un flujo no transmite datos personales, la empresa deberá inventariar payloads por integración, aplicar y probar minimización o desidentificación, revisar archivos y memorias, comprobar segregación entre cuentas, verificar retención y entrenamiento de los proveedores y documentar incidentes de envío accidental. No basta con advertencias al usuario o instrucciones al modelo. EDUAI gestiona datos de cuentas y evaluaciones por vías separadas sujetas a obligaciones de privacidad.

---

06. Solicitudes ARCOP y consentimiento

1. Recibir solicitudes por contacto@innova-space-edu.cl o canal institucional asignado; registrar folio, fecha y responsable.
2. Verificar identidad de forma proporcional y representación cuando proceda, sin solicitar información sensible innecesaria.
3. Determinar si Innova es responsable o encargado; en este último caso, derivar prontamente al responsable y asistir técnicamente.
4. Localizar registros y aplicar, cuando proceda, acceso, rectificación, supresión, oposición, portabilidad o revocación; verificar copias y sistemas relacionados.
5. La Ley reformada prevé respuesta del responsable hasta 30 días corridos, prorrogables una sola vez por 30; las peticiones de bloqueo temporal relacionadas con rectificación, supresión u oposición tienen reglas especiales, incluido el plazo de 2 días hábiles del artículo 11.
6. Guardar constancia de resolución, respuesta, fecha y posibles reclamaciones; no enviar datos por correo sin comprobar destinatario.

---

07. Manejo de incidentes y brechas

1. **Detectar y clasificar:** accesos improcedentes, phishing, claves expuestas, almacenamiento abierto, pérdida de documentos, fuga por IA, errores de RLS o divulgación de datos.
2. **Contener:** revocar credenciales comprometidas, restringir acceso y detener publicaciones o integraciones afectadas, evitando destruir evidencias.
3. **Registrar:** fecha, sistemas, categorías y número estimado de afectados, origen, acciones, responsables, riesgos y versiones.
4. **Comunicar al responsable:** de inmediato y sin dilación indebida; un objetivo operativo contractual propuesto es alerta inicial dentro de 24 horas de detección, sujeto al DPA.
5. **Evaluar notificación legal:** el responsable determina conforme al artículo 14 sexies si debe informar a la Agencia y a titulares. La reforma no establece para todos los casos una regla universal de 72 horas; aplica el estándar legal correspondiente.
6. **Recuperar y mejorar:** corregir causa, probar restauración, verificar eliminación de exposición y documentar lecciones aprendidas.

---

08. Seguridad técnica mínima verificable

Control	Prueba que debe archivarse de forma privada	Frecuencia sugerida
RLS y autorización	Pruebas de acceso cruzado estudiante/docente/institución y políticas SQL revisadas.	En cada cambio relevante y revisión periódica.
Acceso admin y claves	Lista autorizada, MFA donde corresponda, rotación y revocación.	Trimestral y ante salida/incidente.
Backups y restauración	Supabase Free no incluye respaldo automático garantizado ni PITR. Definir exportación programada segura y copia externa de PostgreSQL y objetos Storage; registrar prueba de recuperación, cifrado y RPO/RTO acordados.	Periodicidad según riesgo contractual.
Almacenamiento y enlaces	Clasificación de buckets, pruebas de URL, acceso público/privado.	Al crear bucket o ruta y en auditorías.
Proveedores y contratos	DPA, región, subencargados, cláusulas internacionales, fecha de aprobación.	Antes de activar y al modificar servicio.

Control	Prueba que debe archivarse de forma privada	Frecuencia sugerida
Conservación y borrado	Plazos aprobados, tareas de supresión, respaldo de ejecución.	Programada y al término de contrato.

08-A. Respaldo interno y recuperación: procedimiento de adopción

La empresa proyecta infraestructura propia con un medio externo cifrado inicial para custodiar copias de EDUAI y Sello Tecnológico. Su disponibilidad no acredita que exista un sistema de respaldos operativo ni modifica el almacenamiento principal en Supabase Free. Antes de habilitar este sistema se debe:

1. **Medir y clasificar:** inventariar tamaño real de PostgreSQL, Auth, Storage, anexos, exportaciones e índices; estimar crecimiento por ciclo escolar y conservación legítima, y definir límites de ocupación y alertas.
2. **Preparar el medio:** comprobar estado del disco, sistema de archivos, montaje persistente mediante identificador estable, cifrado y protección de claves independiente, permisos administrativos y restricciones de acceso.
3. **Respaldar por separado:** exportación consistente de base de datos con herramientas soportadas; copia cifrada de objetos Storage desde API o protocolo autorizado; guardar manifiesto con fecha, proyecto, categorías, hashes, integridad y versión. No publicar archivos o secretos en GitHub.
4. **Programar:** esquema de respaldo diario inicial sujeto a validación, histórico con rotación proporcional al tamaño y alertas por fallos. Si supera capacidad, no eliminar el único punto recuperable sin autorización y una copia alternativa verificada.
5. **Independencia:** una segunda copia cifrada desconectada o fuera del lugar principal resulta necesaria para responder a robo, daño físico, malware o corte prolongado. No declarar conformidad con la regla 3-2-1 antes de cumplirla.
6. **Probar:** restauración aislada antes de producción y periódica (objetivo mensual a validar); comprobar acceso mínimo, relaciones, objetos, permisos y ausencia de datos indebidamente restaurados; documentar RPO/RTO reales.
7. **Depurar:** mantener reglas de expiración de copias y registro mínimo de eliminaciones, aplicar supresiones tras restauración, registrar excepciones legales y reportar las purgas de respaldos.
8. **Separar funciones:** el administrador técnico ejecuta; el responsable institucional autoriza conservación/eliminación; la empresa controla claves y accesos. Auditar cambios de configuración y alertas de fallos.

La capacidad nominal del disco no es igual al espacio disponible y no debe utilizarse para calcular plazos fijos de conservación sin conocer el volumen de datos. Las copias bajo custodia propia también constituyen tratamiento sujeto a seguridad, transparencia, responsabilidades y plazos de la Ley 21.719.

---

09. Evaluación de impacto y revisión jurídica

Antes de tratamientos nuevos de alto riesgo evaluar necesidad, proporcionalidad, riesgos y mitigaciones. La ley contempla supuestos como tratamiento a gran escala, perfilados de efectos significativos, monitoreo de lugares públicos y casos de tratamiento de datos sensibles especialmente protegidos. En estudiantes, no basta con el argumento de finalidad educativa para omitir evaluaciones.

---

10. Gestión de subencargados y transferencias

1. Identificar razón social exacta de cada proveedor y producto usado (Supabase, Vercel, Cloudflare, IA, correo y otros, solo donde corresponda).
2. Solicitar y guardar DPA vigente, términos del servicio, políticas de retención, medidas de seguridad y documentos de subprocesadores.
3. Determinar países y garantías de transferencia internacional; documentar autorización específica y escrita del responsable para cada delegación que proceda.
4. Mantener un registro de nuevas integraciones o cambios y bloquear datos sensibles hasta autorizar legal y técnicamente.

---

11. Protocolo operativo de cierre de año escolar

Responsable institucional: fija y aprueba fecha de cierre, finalidades que concluyen, excepciones obligatorias y personas legitimadas para exportar datos. **Innova Space Edu SpA:** ejecuta exportación, supresión y evidencias conforme a sus instrucciones documentadas cuando actúa como encargada.

1. **Preparación:** por colegio, seleccionar ciclo, módulos, tablas, buckets, cuentas, expedientes, sistemas externos, trabajos pendientes, plazos de proveedor, custodia de notas y obligaciones normativas; obtener autorización escrita.
2. **Al menos 30 días antes:** notificar por canales institucionales a usuarios y, cuando corresponda, padres, madres, apoderados y tutores legales. Incluir fecha de cierre, categorías sujetas a eliminación, excepciones, acceso a descarga, contactos y procedimiento de consultas.
3. **Al menos 7 días antes:** enviar recordatorio y comprobar posibilidad de descarga en formatos utilizables, con autorización y registro de los accesos.
4. **En la fecha de cierre:** suspender edición del ciclo cerrado, preparar exportación institucional autorizada, evitar divulgaciones y verificar solicitudes de derechos, reclamaciones o medidas de conservación pendientes.
5. **Dentro de 30 días posteriores:** tras validación del responsable, borrar o anonimizar datos elegibles de bases activas y objetos almacenados. Conservar únicamente cuentas mínimas que deban continuar y registros exceptuados con finalidad/base documentada.
6. **Respaldos, cachés y proveedores:** dado el plan Free de Supabase, asegurar previamente respaldo propio documentado y probado, cuando sea necesario para continuidad o conservación legal; separar exportación de base de datos y de objetos Storage, protegerlos con cifrado y acceso mínimo, y asignar fecha de expiración. Verificar la retención real de copias operacionales de terceros antes de prometer borrado definitivo; registrar la purga y evitar reintroducir datos suprimidos al restaurar copias.

7. **Cierre auditado:** emitir acta con ciclo, institución, categorías, registros/objetos afectados, procedimiento, autorizaciones, incidentes, excepciones, ubicación del backup y evidencias técnicas sin revelar datos personales.

Prohibiciones: no efectuar eliminación masiva directamente sin prueba en ambiente controlado, respaldo válido de elementos legalmente retenibles, evaluación de relaciones entre tablas y aprobación institucional. No confundir aviso con consentimiento. No eliminar registros oficiales requeridos para actas, certificados, obligaciones legales o procedimientos pendientes.

---

12. Calendario de adopción propuesto

1. **Inventario:** mapear tablas, API, buckets, proveedores, flujos y campos realmente tratados.
2. **Contratos:** completar y firmar DPA por institución; verificar anexos de subencargados.
3. **Seguridad:** corregir brechas de acceso, publicación y retención detectadas en la evaluación.
4. **Transparencia:** aprobar política con los 12 contenidos del artículo 14 ter y mantener enlaces públicos accesibles.
5. **Pruebas:** ejercicio de solicitud de derechos, simulación de incidente y recuperación.
6. **Gobernanza:** nombrar responsables, controlar versiones y documentar revisiones al menos cuando cambien riesgos o tecnologías.

Referencias normativas: Ley 21.719, artículos 11, 14 ter, 14 quáter, 14 quinquies, 14 sexies, 15 bis, 15 ter y 16 quáter. Este resumen público no expone medidas técnicas internas ni sustituye actas y procedimientos restringidos.

---

13. Estado de mantenimiento, voz administrativa y pagos suspendidos

1. **Video Studio (E14):** mostrar aviso de mantenimiento y bloquear en servidor nuevas generaciones gratuitas, premium o con credenciales personales, procesamiento de cola y solicitudes directas. Conservar consulta de trabajos anteriores sin reactivar proveedores. Registrar evidencia de pruebas tras cada despliegue.
2. **Pagos y créditos (E17):** mantener `payments_enabled` y `premium_video_enabled` desactivados durante mantenimiento, verificar que los endpoints de nuevas órdenes y pagos rechacen solicitudes. No borrar órdenes existentes; conciliar únicamente operaciones históricas, devoluciones o contracargos que procedan. No capturar números completos de tarjetas. Completar DPA/PSP y plazo R14 antes de reabrir.
3. **Clonación vocal (E13):** solo administración específicamente autorizada; bloquear usuarios no administradores menores y adultos tanto en UI como API, pasarelas de audio y RLS, y registrar pruebas de privilegios negativos. El PR #245 aún no fusionado no acredita operación segura. Separar clonación de la transcripción y síntesis de voz no biométrica genérica.
4. **Actas y autorizaciones:** registrar decisión específica por finalidad y versión, usuario, fecha/hora y evidencias mínimas de representación legal. No pedir de nuevo consentimientos aceptados vigentes en cada sesión; revisar

la vigencia ante cambios materiales. Restringir acceso de menores sin autorización válida; jamás tratar un borrador ficticio como consentimiento real.

La puesta en marcha definitiva requiere pruebas verificables, aprobación documentada y sincronización del RAT, política, DPA y expediente privado. Consultar estado E13–E17.
