Esta traducción se facilita por conveniencia. La versión inglesa es el texto jurídicamente vinculante y prevalece en caso de cualquier discrepancia. English (PDF)

Acuerdo de encargo de tratamiento

conforme al artículo 28 del Reglamento (UE) 2016/679 (RGPD) y al artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) — entre el titular de la licencia (el «Responsable») y Eco Heroes International SL (el «Encargado»)

Partes y funciones

Responsable: _____ (denominación del centro educativo, grupo de centros, administración educativa, empresa u hotel indicado en la Licencia), con domicilio social en _____, representado por _____ (nombre, cargo).
Contacto del Responsable para protección de datos (contacto administrador o, si se ha designado, delegado de protección de datos): _____.

Encargado: Eco Heroes International SL, CIF B44915940, con domicilio social en 17003 Girona (España), inscrita en el Registro Mercantil de Girona, representada por Karim Zouhdi, fundador. Contacto para protección de datos: info@eco-heroes.org, +34 690 814 215. Avisos de seguridad: security@eco-heroes.org (véase https://eco-heroes.org/.well-known/security.txt).

Funciones. El Responsable decide para qué y cómo se tratan los Datos del Responsable y es su responsable del tratamiento. El Encargado trata los Datos del Responsable únicamente por cuenta del Responsable, como encargado del tratamiento en el sentido del artículo 4.8 del RGPD.

Cuentas de docentes. Cada docente tiene una cuenta personal y nominativa. El Encargado gestiona la cuenta en sí (acceso, seguridad, verificación en dos pasos y los recursos gratuitos para docentes) como responsable del tratamiento, conforme a su Política de privacidad. Todo lo que un docente hace en el Servicio para el Responsable son Datos del Responsable: el rol y los permisos de la cuenta en el centro del Responsable, las clases, el alumnado, el progreso, las tareas, los cuestionarios en directo, las importaciones de listas de clase, los accesos desde la plataforma de aprendizaje y los estudios de impacto.

Fuera de este Acuerdo. El anexo I, sección B, enumera los tratamientos de los que el Encargado es responsable por sí mismo. Esos tratamientos se rigen por la Política de privacidad del Encargado (https://eco-heroes.org/legal/privacy/), no por este Acuerdo. Eco Heroes Academy (learn.eco-heroes.org) y la evaluación VSME (assessment.eco-heroes.org) son servicios distintos, con sus propias condiciones e informaciones de privacidad; este Acuerdo no los cubre.

Este Acuerdo forma parte de la Licencia. Si la Licencia y este Acuerdo se contradicen en lo relativo al tratamiento de datos personales, prevalece este Acuerdo.

Definiciones

- **«Licencia»** significa el contrato en virtud del cual el Responsable utiliza el Servicio: el presupuesto o la hoja de pedido aceptados por el Responsable, junto con las Condiciones de licencia para centros educativos y organizaciones publicadas en https://eco-heroes.org/legal/licence/.
- **«Servicio»** significa la plataforma Eco Heroes y el soporte descritos en la cláusula 1.1.
- **«Datos del Responsable»** significa los datos personales que el Encargado trata por cuenta del Responsable en virtud de este Acuerdo, descritos en el anexo I, sección A.
- **«Usuarios»** significa los alumnos, docentes, administradores del centro, empleados, personal, huéspedes y demás personas a las que el Responsable permite utilizar el Servicio.
- **«Subencargado»** significa otro encargado del tratamiento al que el Encargado recurre para tratar Datos del Responsable.
- **«Día hábil»** significa de lunes a viernes, excepto los días festivos en Girona (España).
- Los términos definidos en el artículo 4 del RGPD, como «datos personales», «tratamiento» y «violación de la seguridad de los datos personales», tienen en este Acuerdo el mismo significado.

1. Objeto y duración

1.1 El Encargado presta el Servicio al Responsable en virtud de la Licencia. El Servicio comprende: el juego de aventuras, el trivial, los juegos de palabras y los cuestionarios de clase en directo; los libros ilustrados y la Story Library, los vídeos de las misiones, los manuales y los planes de clase; cuentas nominativas de docentes, gestión de clases y tareas; la importación opcional de listas de clase (CSV, CSV OneRoster, Google Classroom); el acceso opcional de docentes con Google o Microsoft; la conexión opcional con la plataforma de aprendizaje del Responsable mediante LTI 1.1 o LTI 1.3; el panel de clase de la aplicación móvil Eco Heroes, cuando el Responsable lo utilice; los estudios de impacto opcionales; en las licencias para empresas y hoteles, cuentas de coordinador, grupos con códigos de acceso para los hijos de los empleados o de los huéspedes e informes de progreso por grupo (CSV), un informe agregado de la organización, certificados con el nombre de la organización e inicio de sesión opcional del personal con el proveedor de identidad del propio Responsable; y el soporte.

1.2 El Encargado trata los Datos del Responsable durante la vigencia de la Licencia y hasta que todos los Datos del Responsable se hayan suprimido o devuelto conforme a la cláusula 10.

2. Naturaleza y finalidad del tratamiento; categorías

2.1 El **anexo I** recoge la naturaleza y la finalidad del tratamiento, las categorías de interesados y las categorías de datos personales.

2.2 El Encargado trata los Datos del Responsable únicamente para prestar el Servicio al Responsable. No los utiliza para publicidad, para elaborar perfiles del alumnado más allá del progreso de aprendizaje que el Servicio muestra a los docentes del Responsable, para vender o ceder datos, ni para desarrollar ningún producto distinto del Servicio.

2.3 **Estadísticas anonimizadas.** Cuando el Responsable inscribe clases en un estudio de impacto, instruye al Encargado para que elabore estadísticas agregadas a partir de las respuestas, que el Encargado puede utilizar en sus propios informes y publicaciones. El Encargado solo agrega respuestas de grupos de al menos 10 alumnos, nunca incluye respuestas de texto libre y comprueba que no pueda identificarse a ningún alumno, clase ni centro. Las estadísticas así elaboradas ya no son datos personales. El Responsable puede retirar esta instrucción en cualquier momento mediante aviso

por escrito; las respuestas recogidas a partir de entonces solo se utilizan para los resultados propios del Responsable.

3. Instrucciones

3.1 El Encargado trata los Datos del Responsable únicamente siguiendo instrucciones documentadas del Responsable, también en lo relativo a las transferencias a un tercer país o a una organización internacional, salvo que el Derecho de la Unión o de los Estados miembros que se aplique al Encargado le obligue a otra cosa. En tal caso, el Encargado informa al Responsable de esa exigencia legal antes del tratamiento, salvo que dicho Derecho lo prohíba por razones importantes de interés público.

3.2 Constituyen instrucciones documentadas del Responsable este Acuerdo, la Licencia y los ajustes que el Responsable y sus Usuarios elijan en el Servicio (por ejemplo, crear clases, importar listas de clase, activar el acceso único o la conexión con una plataforma de aprendizaje, inscribir una clase en un estudio de impacto, eliminar alumnos o clases). El contacto administrador del Responsable da cualquier otra instrucción por escrito; basta un correo electrónico a info@eco-heroes.org.

3.3 El Encargado informa inmediatamente al Responsable si, en su opinión, una instrucción infringe el RGPD, la LOPDGDD u otras disposiciones de protección de datos de la Unión o de los Estados miembros. El Encargado puede suspender esa instrucción hasta que el Responsable la confirme o la modifique.

4. Obligaciones del Responsable

4.1 El Responsable responde de la licitud del tratamiento, incluida la base jurídica para tratar los datos del alumnado; de facilitar a los interesados la información exigida por los artículos 13 y 14 del RGPD (alumnado y, en su caso, sus madres, padres o tutores, docentes, administradores, empleados y huéspedes); de obtener el consentimiento que exija la ley aplicable al Responsable para el alumnado que no haya alcanzado la edad de consentimiento digital (artículo 8 del RGPD; artículo 7 de la LOPDGDD: 14 años en España); y de la exactitud de los datos que él y sus Usuarios introduzcan.

4.2 El Responsable indica a sus Usuarios que no introduzcan categorías especiales de datos personales (artículo 9 del RGPD), apellidos, direcciones de correo electrónico ni otros identificadores directos del alumnado en campos de texto libre, como apodos, nombres de clase, notas de tareas, apodos de cuestionarios en directo y respuestas a encuestas.

4.3 Cuando el Responsable conecta su propia plataforma de aprendizaje (LTI) o su proveedor de identidad (acceso único), el Responsable responde de ese sistema y de configurarlo para que comparta únicamente los datos descritos en el anexo I (en el caso del alumnado por LTI, solo el nombre y nunca la dirección de correo electrónico).

4.4 El Responsable designa un contacto administrador y, antes de realizar un estudio de impacto, un contacto de protección de la infancia, y mantiene ambos actualizados en el Servicio o mediante correo electrónico al Encargado. Mientras no se designe un contacto de protección de la infancia, o mientras la cuenta del contacto designado esté cerrada, el Servicio traslada los avisos de protección de la infancia a los administradores del centro del Responsable. En las clases que no están vinculadas a un centro en el Servicio (por ejemplo, clases que solo se usan mediante un lanzamiento LTI), los avisos llegan a la persona responsable de protección de la infancia del Encargado, que los traslada sin demora al contacto administrador del Responsable.

5. Obligaciones del Encargado

El Encargado:

a. tratará los Datos del Responsable únicamente conforme a la cláusula 3;

b. garantizará que toda persona autorizada para tratar Datos del Responsable esté sujeta a confidencialidad, por contrato o por ley, y que el acceso a los sistemas de producción se limite a personas identificadas que lo necesiten;

c. aplicará las medidas técnicas y organizativas del **anexo II** y mantendrá un nivel de seguridad adecuado al riesgo conforme al artículo 32 del RGPD, teniendo en cuenta que entre los interesados hay menores;

d. recurrirá a otro encargado solo en los términos de la cláusula 6;

e. teniendo en cuenta la naturaleza del tratamiento, asistirá al Responsable mediante medidas técnicas y organizativas apropiadas, siempre que sea posible, para responder a las solicitudes de ejercicio de derechos de los interesados (artículos 12 a 23 del RGPD), según se establece en la cláusula 8;

f. ayudará al Responsable a cumplir los artículos 32 a 36 del RGPD (seguridad, notificación de violaciones, evaluación de impacto relativa a la protección de datos, consulta previa), teniendo en cuenta la naturaleza del tratamiento y la información a disposición del Encargado; el resumen de la evaluación de impacto vigente del Encargado está publicado en el Centro de confianza y la evaluación completa está a disposición del Responsable previa solicitud;

g. a elección del Responsable, suprimirá o devolverá todos los Datos del Responsable al finalizar el Servicio y suprimirá las copias existentes, salvo que el Derecho de la Unión o de los Estados miembros exija conservarlos (cláusula 10);

h. pondrá a disposición del Responsable toda la información necesaria para demostrar el cumplimiento del artículo 28 del RGPD, y permitirá y contribuirá a la realización de auditorías, incluidas inspecciones, por parte del Responsable o de un auditor mandatado por él (cláusula 11);

i. llevará un registro de las categorías de actividades de tratamiento efectuadas por cuenta del Responsable (artículo 30.2 del RGPD);

j. transferirá Datos del Responsable a un tercer país solo en los términos de la cláusula 7.

6. Subencargados

6.1 El Responsable otorga una autorización general por escrito para los Subencargados enumerados en el **anexo III, parte A**.

6.2 El Encargado informa al Responsable de toda incorporación o sustitución prevista de un Subencargado con al menos **30 días** de antelación, mediante correo electrónico al contacto administrador del Responsable y actualizando https://eco-heroes.org/trust/. El Responsable puede oponerse por motivos razonables relacionados con la protección de datos. Si la oposición no puede resolverse en el plazo de preaviso, el Responsable puede resolver la parte afectada de la Licencia sin penalización, y se aplica la cláusula 10.

6.3 El Encargado recurre a cada Subencargado conforme a las condiciones estándar de tratamiento de datos de ese proveedor. Dichas condiciones obligan al Subencargado a cumplir obligaciones de protección de datos que ofrecen garantías suficientes de medidas técnicas y organizativas apropiadas, como exige el artículo 28.4 del RGPD. El Encargado sigue siendo plenamente responsable ante el Responsable del cumplimiento de esas obligaciones por cada Subencargado.

6.4 El **anexo III, parte B** enumera servicios de terceros que el Encargado utiliza pero que **no** tratan Datos del Responsable. No tratan datos personales, o solo tratan datos de los que el Encargado es

responsable. Se enumeran por transparencia y no son Subencargados a efectos de este Acuerdo.

6.5 Los sistemas propios del Responsable, como su plataforma de aprendizaje o su entorno de Google o Microsoft, los elige y controla el Responsable. No son Subencargados del Encargado.

7. Transferencias internacionales

7.1 Los Datos del Responsable se alojan y almacenan en la Unión Europea: los servidores de aplicación, en Francia (Internet Girona, sobre infraestructura de OVHcloud); la base de datos, las copias de seguridad cifradas y un servidor de reserva, en Alemania y Finlandia (Hetzner Online GmbH). La red de distribución de contenidos (Cloudflare) sirve páginas públicas en caché desde su red mundial. Las respuestas que contienen datos personales se marcan como privadas y no almacenables (no-store), y la red no las almacena en caché.

7.2 El Encargado no transfiere Datos del Responsable fuera del Espacio Económico Europeo, ni permite que un Subencargado lo haga, salvo (i) cuando el destino cuente con una decisión de adecuación de la Comisión Europea, incluidas Suiza y, para las organizaciones cuya certificación el Encargado haya comprobado en la lista oficial, el Marco de Privacidad de Datos UE-EE. UU.; o (ii) sobre la base de las cláusulas contractuales tipo adoptadas por la Decisión de Ejecución (UE) 2021/914 de la Comisión (módulo 3, de encargado a encargado, o módulo 2 cuando proceda), con medidas adicionales cuando una evaluación de la transferencia muestre que son necesarias. El anexo III indica la garantía aplicable a cada Subencargado. El Encargado mantiene por escrito una evaluación de la transferencia para cada Subencargado situado fuera del EEE y la pone a disposición del Responsable previa solicitud.

7.3 Cloudflare, Inc. termina la conexión cifrada en su red perimetral, por lo que allí trata datos de la solicitud (dirección IP, dirección solicitada, cabeceras). El Encargado se basa en las condiciones estándar de tratamiento de datos de Cloudflare con las cláusulas contractuales tipo y, cuando Cloudflare figure en la lista oficial del Marco de Privacidad de Datos, en el Marco de Privacidad de Datos UE-EE. UU.

7.4 Proton AG aloja el correo electrónico del Encargado en Suiza. Suiza cuenta con una decisión de adecuación de la Comisión Europea.

8. Asistencia en el ejercicio de derechos

8.1 Los docentes pueden consultar, exportar (CSV), renombrar, restablecer y eliminar los datos de un alumno, y eliminar clases completas, directamente en el Servicio. Cada docente ve solo sus propias clases; los administradores del centro ven todas las clases de su centro y pueden retirar de inmediato el acceso de un docente. El Responsable utiliza estas funciones para atender las solicitudes siempre que pueda.

8.2 Cuando una solicitud no pueda atenderse mediante el Servicio, el Encargado asiste al Responsable en un plazo de **10 días hábiles** desde una solicitud por escrito. Si el Encargado recibe directamente de un interesado (incluidos madres, padres o tutores) una solicitud relativa a Datos del Responsable, no la resuelve en cuanto al fondo. Remite al interesado al Responsable sin dilación indebida e informa al Responsable, salvo que este le indique otra cosa.

9. Violación de la seguridad de los datos personales

9.1 El Encargado notifica al Responsable toda violación de la seguridad de los datos personales que afecte a Datos del Responsable sin dilación indebida y, a más tardar, en un plazo de **48 horas** desde

que tenga conocimiento de ella. La primera notificación contiene la información exigida por el artículo 33.3 del RGPD en la medida en que se conozca en ese momento: la naturaleza de la violación, las categorías y el número aproximado de interesados y de registros afectados, las consecuencias probables y las medidas adoptadas o propuestas. El Encargado completa la información por fases a medida que disponga de ella.

9.2 El Encargado colabora con el Responsable para investigar, contener y documentar la violación, y le ayuda en cualquier notificación a la autoridad de control (en España, la Agencia Española de Protección de Datos) y en cualquier comunicación a los interesados. El Encargado documenta toda violación de la seguridad de los datos personales, incluidos los hechos, sus efectos y las medidas adoptadas.

9.3 El Encargado envía las notificaciones por correo electrónico al contacto administrador del Responsable. Cualquier persona puede comunicar una vulnerabilidad de seguridad a security@eco-heroes.org. Se acusa recibo de las comunicaciones en un plazo de 5 días hábiles y los problemas críticos se corrigen antes que cualquier otro trabajo.

10. Conservación, supresión y devolución

10.1 **Durante la Licencia.** Los Datos del Responsable se conservan conforme al calendario del anexo I, sección C, que refleja las reglas de conservación aplicadas en el código del Servicio. Un docente puede eliminar un alumno o una clase en cualquier momento, con efecto inmediato en la base de datos activa y en la réplica de reserva.

10.2 **Exportación.** Durante la Licencia, y hasta la supresión conforme a la cláusula 10.3, el Responsable puede exportar en el Servicio los datos de clase y de progreso en formato CSV, o pedir al Encargado una exportación en un formato estructurado, de uso común y de lectura mecánica.

10.3 **Fin de la Licencia.** Si la Licencia termina y no se renueva, el Encargado suprime los Datos del Responsable **90 días** después de la fecha de finalización. Si el Responsable lo solicita por escrito, el Encargado suprime los Datos del Responsable en un plazo de **30 días** desde la solicitud, haya terminado o no la Licencia. El Encargado confirma la supresión por escrito previa solicitud. Antes de la supresión, el Encargado envía un correo electrónico a los administradores del centro del Responsable 30 días y 7 días antes de la fecha de supresión, en el que indica esa fecha y cómo renovar la Licencia o exportar los datos; la supresión no se produce antes de que hayan transcurrido 30 días desde el primer mensaje y 7 días desde el segundo.

10.4 **Cuentas de docentes.** Cuando termina la última licencia vinculada a una cuenta de docente, la cuenta continúa como cuenta gratuita de docente. Se suprime 12 meses después de la finalización de esa licencia, salvo que entretanto el docente se vincule a una nueva licencia; una cuenta gratuita se suprime tras 12 meses sin inicio de sesión. El Encargado envía un correo electrónico al docente 30 días antes de la supresión. Mantener una cuenta de docente no conserva ningún Dato del Responsable: esos datos se suprimen conforme a la cláusula 10.3.

10.5 **Copias de seguridad y réplica.** Los datos suprimidos desaparecen de las copias de seguridad en el ciclo ordinario. Las copias de seguridad cifradas se conservan de forma rotatoria, de modo que los datos suprimidos desaparecen de todas ellas en un plazo de **14 días**. La réplica de solo lectura del servidor de reserva sigue cada supresión de forma continua. Las copias de seguridad solo se restauran para recuperarse de una pérdida del sistema de producción; si una restauración recupera datos suprimidos, la supresión se aplica de nuevo.

10.6 **Conservación legal.** El Encargado conserva datos personales tras el fin de la Licencia solo cuando y durante el tiempo que lo exija el Derecho de la Unión o de los Estados miembros, por ejemplo las

facturas y los registros contables durante 6 años conforme al artículo 30 del Código de Comercio. Estos registros identifican a las personas de contacto del Responsable y no contienen datos del alumnado. El Encargado los protege conforme al anexo II y no los utiliza para ninguna otra finalidad.

11. Auditoría e información

11.1 Previa solicitud, y como máximo una vez por año contractual (o además tras una violación de la seguridad de los datos personales o ante una sospecha documentada y razonable de incumplimiento), el Encargado facilita al Responsable la información necesaria para demostrar el cumplimiento de este Acuerdo. Esta incluye el resumen de seguridad vigente (https://eco-heroes.org/trust/#security), la lista vigente de Subencargados, el registro de los tratamientos efectuados por cuenta del Responsable, las evaluaciones de las transferencias, la evaluación de impacto relativa a la protección de datos, los últimos resultados de las pruebas de restauración y de los ensayos de conmutación por error y los resultados de cualquier revisión de seguridad.

11.2 Si esta información no basta, el Responsable, o un auditor independiente mandatado por él y sujeto a confidencialidad, puede auditar los tratamientos pertinentes del Encargado con un preaviso de al menos **30 días**, en horario laboral y sin perturbar de forma irrazonable las operaciones del Encargado ni a otros clientes. Cada parte asume sus propios costes. El Encargado puede pedir al auditor que firme un compromiso de confidencialidad razonable y puede limitar el acceso a sistemas compartidos con otros clientes a lo necesario para verificar el cumplimiento.

12. Responsabilidad

12.1 Cada parte responde ante los interesados conforme al artículo 82 del RGPD. Entre las partes, la responsabilidad se rige por la cláusula de responsabilidad de la Licencia. Nada en este Acuerdo ni en la Licencia limita la responsabilidad de una parte cuando la ley no permita limitarla, incluida la responsabilidad por dolo.

12.2 Si el Encargado tiene que pagar una multa administrativa o una indemnización a causa de las instrucciones del Responsable o porque el Responsable no cumplió sus obligaciones de la cláusula 4, el Responsable mantendrá indemne al Encargado en la medida de esa causa, y lo mismo se aplica a la inversa.

13. Vigencia, ley aplicable y jurisdicción

13.1 Este Acuerdo entra en vigor en la fecha de inicio de la Licencia y termina cuando todos los Datos del Responsable se hayan suprimido o devuelto conforme a la cláusula 10. Las cláusulas 5(b), 10, 11 y 12 siguen aplicándose durante el tiempo necesario.

13.2 Este Acuerdo se rige por el Derecho español y el Derecho de la Unión Europea, incluidos el RGPD y la LOPDGDD. Son competentes los juzgados y tribunales de Girona (España), sin perjuicio de las normas imperativas aplicables al Responsable como entidad pública o en virtud de la normativa de contratación pública, y sin perjuicio de los derechos de los interesados conforme al artículo 79 del RGPD. El anexo V añade las reglas para responsables en el Reino Unido y en los Estados Unidos.

13.3 Las modificaciones de este Acuerdo deben hacerse por escrito; basta el correo electrónico. El Encargado publica el modelo vigente en https://eco-heroes.org/trust/. Una nueva versión del modelo no modifica un Acuerdo firmado salvo que el Responsable lo acepte. El administrador del centro del Responsable puede aceptar este Acuerdo en línea; el Encargado registra quién lo aceptó, cuándo, qué versión y un hash con clave de la dirección IP utilizada.

Firmas

Por el Responsable

Nombre, cargo
Fecha, firma

Por el Encargado — Eco Heroes International SL

Karim Zouhdi, fundador
Fecha, firma

Anexo I — Detalles del tratamiento

A. Tratamiento por cuenta del Responsable (ámbito de este Acuerdo)

Anexo I.A — tratamiento por cuenta del Responsable

Elemento	Descripción
Objeto	Prestación del Servicio a los Usuarios del Responsable en virtud de la Licencia.
Naturaleza	Alojamiento, almacenamiento, visualización y supresión de datos; seguimiento del progreso; cuestionarios de clase en directo; tareas; certificados; gestión de clases; importación opcional de listas de clase facilitadas por el Responsable (pegado o carga de CSV, CSV OneRoster 1.1/1.2, Google Classroom); accesos opcionales LTI 1.1 / LTI 1.3 desde la plataforma de aprendizaje del Responsable, con aprovisionamiento de nombres y roles (importación de listas) y servicios de tareas y calificaciones (envío de puntuaciones); acceso opcional de docentes con Google o Microsoft elegido por el Responsable; el panel de clase de la aplicación móvil Eco Heroes cuando el Responsable reparte un código de clase; cuestionarios opcionales de estudios de impacto en las clases que inscriba el Responsable; cuentas de coordinador, códigos de acceso de grupo e informes de progreso por grupo (CSV) en las licencias para empresas y hoteles; soporte. En las licencias de empresa y de hotel, además: informes de actividad agregados para la organización (informe de la organización y totales, con cualquier cifra basada en menos de 5 familias oculta) y una clasificación por equipos opcional; el nombre y el logotipo de la organización en los certificados de los niños; inicio de sesión opcional del personal con el proveedor de identidad del propio Responsable (OpenID Connect).
Finalidad	Impartir educación para la sostenibilidad basada en los Objetivos de Desarrollo Sostenible de la ONU, con la vista de progreso, los informes y la evaluación que incluye la Licencia. En los estudios de impacto: la evaluación por el Responsable de su enseñanza (resultados de clase para sus docentes) y estadísticas agregadas y anonimizadas conforme a la cláusula 2.3. Ninguna otra finalidad.
Categorías de interesados	Alumnado (el juego está concebido para edades de 9 a 17 años en dos franjas, 9-12 y 13-17; los planes de clase imprimibles abarcan las franjas 6–10, 11–13 y 14–17 años, y el Responsable puede utilizar el Servicio con alumnado más joven bajo su propia valoración); docentes; administradores del centro; madres, padres y tutores, solo cuando se utilice el procedimiento de consentimiento; en las licencias para empresas y hoteles, los hijos de los empleados o de los huéspedes y los coordinadores de la organización.
Datos personales — alumnado (sitio web, en una clase)	Nombre o apodo escrito por el alumno o introducido por el docente (de 2 a 24 caracteres; en las importaciones de listas, el nombre de pila más la inicial, ampliada como máximo a las 3 primeras letras del apellido solo para distinguir a dos alumnos con el mismo nombre, nunca el apellido completo); franja de edad elegida en el juego (9-12 o 13-17); avatar de un conjunto fijo; idioma; progreso (puntos, objetivos y misiones completados, estrellas del trivial, número de preguntas respondidas y acertadas por tema); tareas completadas; fecha de alta y de última actividad; un identificador aleatorio de clase guardado en el dispositivo del alumno para poder guardar el progreso. En un cuestionario de clase en directo: el apodo introducido, las respuestas, los tiempos de respuesta y la puntuación. No se recogen: dirección de correo electrónico, apellidos, fotografía, fecha de nacimiento, dirección postal, ubicación, identificadores del dispositivo ni publicitarios.

Elemento	Descripción
Datos personales — alumnado (accesos LTI)	Un hash con clave del identificador de usuario de la plataforma (para asociar a un alumno con una plaza); el identificador de usuario de la plataforma en el registro de acceso durante 90 días, solo cuando la plataforma haya concedido el servicio de calificaciones (necesario para enviar la puntuación); nombre de pila más inicial del apellido como apodo; identificador y título del curso; roles; configuración regional; última puntuación enviada. No se almacena ninguna dirección de correo electrónico ni ningún nombre completo; el Responsable configura su plataforma para que comparta solo el nombre.
Datos personales — alumnado (aplicación móvil, panel de clase)	Actividad (juego diario jugado, fecha, idioma, puntos, finalización, duración; objetivos alcanzados, insignias) y un hash unidireccional de un identificador aleatorio de instalación generado por la aplicación. El alumnado aparece ante el docente con un alias generado. El panel no muestra nada en una clase con menos de cinco alumnos activos.
Datos personales — alumnado (estudio de impacto, cuando el Responsable inscribe una clase)	Respuestas al cuestionario del estudio (opciones, valoraciones y respuestas breves opcionales de texto libre), versión del cuestionario, idioma, franja de edad, hora de inicio y de envío e indicadores de calidad. Las direcciones de correo electrónico y los números de teléfono se eliminan del texto libre al recibirlo. Las respuestas que puedan contener una revelación relevante para la protección de la infancia se señalan al contacto de protección de la infancia designado por el Responsable. Las respuestas se vinculan entre las rondas del estudio mediante un hash unidireccional con clave de la plaza del alumno en la clase; no se recoge nombre, dirección de correo electrónico ni fecha de nacimiento. Para cada plaza, la exclusión o el consentimiento por escrito que registre el Responsable. Si no se ha designado un contacto de protección de la infancia, los destinatarios previstos en la cláusula 4.4 ocupan su lugar.
Datos personales — docentes y administradores del centro	Nombre, dirección de correo electrónico profesional, centro, rol (docente o administrador del centro), idioma; contraseña (hash bcrypt) o identificador de acceso único; secreto de verificación en dos pasos y códigos de respaldo en hash si se ha activado (obligatoria para administradores del centro); estado de verificación del correo electrónico; horas y número de inicios de sesión; sesiones; clases creadas; vistas previas de importaciones de listas (solo nombres, guardadas en la sesión durante 30 minutos); entradas del registro de auditoría de acciones administrativas (con un hash con clave de la dirección IP y el país de la conexión en código de 2 letras, facilitado por la red de distribución de contenidos); correspondencia de soporte.
Datos personales — docentes (estudio de impacto)	Respuestas al cuestionario docente y, para alumnado de 6 a 8 años, la hoja de observación de la clase, vinculadas mediante un hash unidireccional con clave de la cuenta o el código del docente; la inscripción de la clase, su modalidad de consentimiento y su asignación a un grupo del estudio.
Datos personales — madres, padres y tutores	Solo cuando se utilice el procedimiento de consentimiento parental del sitio web para un alumno que no haya alcanzado la edad de consentimiento digital: un hash unidireccional con clave de la dirección de correo electrónico del progenitor (la dirección se utiliza una sola vez para enviar el enlace de confirmación y no se almacena), la decisión y sus marcas de tiempo.

Elemento	Descripción
Datos personales — menores y coordinadores (licencias para empresas y hoteles)	Hijos de los empleados o de los huéspedes del Responsable: se unen a un grupo con el código de acceso del Responsable y un nombre de héroe (apodo) en su propio dispositivo o en uno de la familia, sin cuenta y sin dirección de correo electrónico. El Servicio guarda los mismos datos que para el alumnado de una clase: nombre de héroe, franja de edad, avatar, idioma, progreso y resultados de los cuestionarios. Coordinadores: nombre, dirección de correo electrónico de trabajo, contraseña en hash o identificador de acceso, configuración de la verificación en dos pasos y los grupos que abren. El coordinador ve los objetivos completados y los resultados de los cuestionarios por grupo y puede exportarlos en CSV. Para el informe de la organización, el Servicio registra además para cada perfil de héroe de estos grupos los días de actividad y el día en que se completó por primera vez cada objetivo o misión (con precisión de día; las clases de los colegios no se registran así). Los informes contienen solo datos agregados: ningún nombre, apodo, identificador ni fila por niño; cualquier cifra basada en 1 a 4 familias se oculta (k = 5), y se oculta una segunda cifra cuando una sola permitiría deducirla. Los nombres de los equipos los elige el administrador del Responsable y no deben nombrar a personas. Cuando el Responsable activa el inicio de sesión de empresa, los nombres y correos del personal proceden del proveedor de identidad del propio Responsable (ámbitos openid, email y profile); ese proveedor de identidad es un sistema y un encargado del propio Responsable, no un Subencargado, y su identificador de sujeto se guarda solo como hash con clave. Marca compartida: el nombre visible y el logotipo de la organización, facilitados por el Responsable. La página pública de la insignia que una madre, un padre o un tutor puede compartir en LinkedIn no contiene datos personales (un número de objetivos, el nombre de la organización si el Responsable lo ha activado y un idioma, todo tomado de su enlace); la persona adulta inicia el envío y el Encargado no envía nada a LinkedIn.
Categorías especiales (artículo 9 del RGPD)	No se solicitan ni son necesarias. Véase la cláusula 4.2.
Frecuencia	Continua, durante la vigencia de la Licencia.

B. Tratamientos de los que Eco Heroes es responsable independiente (fuera de este Acuerdo)

Se enumeran para que el Responsable vea dónde termina este Acuerdo. Se rigen por la Política de privacidad (v4.3) y el Aviso de privacidad infantil (v2.2) del Encargado, no por este Acuerdo:

- **Las cuentas de docentes en sí:** acceso, seguridad, verificación en dos pasos y recursos gratuitos para docentes. El Encargado es responsable de la cuenta en sí y la suprime según la cláusula 10.4; la actividad de la cuenta para el Responsable son Datos del Responsable.
- **Cuentas gratuitas de docentes:** docentes no vinculados a una licencia que utilizan los recursos gratuitos para docentes con una dirección de correo electrónico verificada.
- **Suscripciones familiares** contratadas en el sitio web por una madre, un padre o un tutor: la dirección de correo electrónico (guardada parcialmente enmascarada), las referencias de pago y de suscripción de Stripe y un código de acceso personal (guardado como hash con clave). Los datos de la tarjeta nunca llegan al Encargado. Un código familiar utilizado en el centro no lleva datos del centro.
- **Cuentas de la aplicación** (acceso de madres y padres con Google o Apple; suscripciones a través de Google Play o Apple; estado de la suscripción a través de RevenueCat).

- **Visitantes del sitio web** en páginas públicas para adultos (Google Analytics 4 tras consentimiento; el formulario de contacto a través de Formspree; las solicitudes de presupuesto y de embajadores a través del propio servidor del Encargado; los correos de Dinner Questions a través de Brevo).
- **Clasificación pública del trivial** (voluntaria: un apodo elegido de una lista generada, la puntuación y un hash con clave de la dirección IP; se conserva 30 días).
- **Encuestas del programa** que el Encargado realiza fuera de una clase, con el consentimiento de la madre, el padre o el tutor cuando la ley lo exija.
- **Servicios distintos:** Eco Heroes Academy (learn.eco-heroes.org) y la evaluación VSME (assessment.eco-heroes.org) tienen sus propias condiciones e informaciones de privacidad.

C. Calendario de conservación (tal como se aplica en el Servicio)

Anexo I.C — calendario de conservación

Datos	Conservación	Mecanismo
Datos del alumnado y de los menores de grupos de empresas y hoteles (apodo, franja de edad, avatar, progreso, tareas, actividad de clase en la aplicación, asociación de plazas LTI)	Durante la Licencia: hasta que un docente o administrador elimine al alumno o la clase. Tras el fin de la Licencia: supresión 90 días después de la fecha de finalización, salvo renovación de la Licencia. A solicitud escrita del Responsable: supresión en un plazo de 30 días; los administradores del centro reciben un aviso por correo electrónico 30 y 7 días antes de la supresión	Acción del docente o administrador en el Servicio; supresión automática al fin de la licencia; el Encargado a solicitud escrita
Fechas de actividad de los perfiles de héroe en grupos de empresa y de hotel (informe de la organización)	Se conservan con el perfil de héroe y se eliminan con él, según la regla anterior	Eliminación con el perfil
Configuración de la organización: nombres de equipos y equipo de cada grupo, activación de la clasificación por equipos, nombre y logotipo de la marca compartida, configuración del inicio de sesión de empresa	Durante la vigencia de la Licencia; se elimina a petición del Responsable	Encargado, a petición
Inicio de sesión de empresa: registros del proceso de inicio de sesión; vínculos de identidad fijados (hash con clave del sujeto del proveedor de identidad)	Registros del proceso: se eliminan al usarse o a los 10 minutos. Vínculos de identidad: hasta que se elimine la cuenta o se elimine o restablezca la configuración de inicio de sesión del Responsable	Purga automática; acción del administrador
Cuestionarios de clase en directo (apodos, respuestas, tiempos, puntuaciones)	30 días desde la creación de la sesión del cuestionario	Depuración diaria automática
Vistas previas de importación de listas (OneRoster)	30 minutos, solo en la sesión del docente en el servidor	Expiración de la sesión
Token de acceso de Google Classroom (importación de listas)	Solo durante la importación, en la sesión del docente; nunca se escribe en la base de datos	Expiración de la sesión

Datos	Conservación	Mecanismo
Registros de accesos LTI	Accesos de docentes y de alumnos sin servicio de calificaciones: 2 horas. Accesos de alumnos con servicio de calificaciones: 90 días	Depuración automática con la actividad LTI
Estado de inicio de sesión LTI, tokens de traspaso, tokens de enlace profundo, nonces, tokens de importación de listas	10 minutos / 10 minutos / 60 minutos / 15 minutos / 2 horas	Depuración automática; un solo uso
Cuentas de docentes, de coordinadores y de administradores del centro	12 meses después del fin de la última licencia vinculada a la cuenta; cuentas gratuitas tras 12 meses sin inicio de sesión; correo de aviso 30 días antes de la supresión. Registros no verificados: se eliminan 7 días después de caducar el último enlace de confirmación	Depuración automática de cuentas
Sesiones y «recordarme»	Sesión del servidor durante su vida útil configurada, renovada al iniciar sesión y cada 30 minutos; todas las sesiones terminan al cambiar la contraseña o cuando un administrador retira el acceso. Cookie «recordarme»: 180 días (firmada con HMAC)	Código
Registros de limitación de frecuencia (intentos de inicio de sesión y otros límites)	30 días	Depuración diaria automática
Registro de auditoría de seguridad (acciones administrativas, activaciones de códigos e inicios de sesión; hash con clave de la IP, país de la conexión en código de 2 letras)	12 meses	Depuración diaria automática
Hashes de IP contra abusos en respuestas a encuestas y solicitudes de consentimiento	30 días (la respuesta sigue su propio plazo)	Depuración diaria automática
Solicitudes de consentimiento parental	Sin respuesta o caducadas: 30 días. Denegaciones: 12 meses. Consentimiento otorgado: mientras se invoque; se borra con los datos al retirarse el consentimiento	Depuración diaria automática; función de borrado
Respuestas de estudios de impacto (alumnado, docentes, hojas de observación) y marcas de exclusión o consentimiento	24 meses tras el cierre de la última ronda del estudio; antes, por instrucción escrita del Responsable. Las marcas de exclusión y consentimiento se suprimen con la inscripción de la clase	Depuración diaria automática; el Encargado a solicitud escrita
Avisos de protección de la infancia (respuestas de estudios de impacto que pueden contener una revelación, con la plaza y el apodo a los que pertenecen)	El texto de la respuesta se borra 30 días después de que el aviso se marque como atendido; el registro del aviso se elimina 12 meses después de atenderse	Depuración diaria automática

Datos	Conservación	Mecanismo
Respuestas a encuestas del programa	24 meses, o hasta que se retire el consentimiento	Depuración diaria automática; función de borrado
Entradas de la clasificación pública del trivial (fuera de este Acuerdo, se incluyen para completar)	30 días	Depuración diaria automática
Registros de la aceptación de este Acuerdo por el Responsable (quién lo aceptó, cuándo, qué versión y un hash con clave de la dirección IP; los conserva el Encargado como responsable, cláusula 13.3)	Mientras dure la Licencia y 6 años después de que termine	Registros del Encargado
Registros de aceptación en el pago, de cancelación y de desistimiento de los planes familiares (fuera de este Acuerdo, se incluyen para completar)	6 años, con los registros contables (Código de Comercio, artículo 30)	Registros contables
Contador de tasa de participación derivado de una persona	2 días	Depuración diaria automática
Telemetría (informes de infracciones de CSP y de errores de JavaScript)	Sin identificadores almacenados (agente de usuario acortado); los contadores de limitación se reinician cada minuto; registro limitado a 5 MB	Código
Correspondencia de soporte (correo electrónico)	Hasta que se atiende la solicitud, y como máximo 12 meses tras el último mensaje	Procedimiento del buzón del Encargado
Copias de seguridad cifradas	Copias cifradas conservadas de forma rotatoria; los datos suprimidos desaparecen de todas las copias en un plazo de 14 días	Automático
Réplica de la base de datos de reserva	Continua; sigue cada supresión	Replicación
Registros técnicos del servidor web (dirección IP, dirección solicitada)	Hasta 90 días	Configuración del servidor
Facturas y registros de pago	6 años (Código de Comercio, artículo 30); identifican a las personas de contacto del Responsable, nunca al alumnado	Registros contables

Anexo II — Medidas técnicas y organizativas (artículo 32 del RGPD)

Las medidas vigentes en la fecha de este Acuerdo. Se revisan con cada versión y el resumen vigente se publica en https://eco-heroes.org/trust/#security. El Encargado puede actualizar las medidas siempre que el nivel general de seguridad no disminuya.

1. Cifrado en tránsito

- TLS 1.2 o superior en todas las conexiones; HTTP Strict Transport Security con max-age de dos años, includeSubDomains y preload; renovación automática de certificados; certificados de origen entre la red de distribución de contenidos y los servidores.
- Los servidores de aplicación se conectan a la base de datos solo mediante TLS 1.2/1.3, con verificación del certificado frente a una autoridad de certificación fijada; la base de datos rechaza las conexiones sin cifrar (require_secure_transport). Las cuentas de la base de datos se limitan a los equipos de aplicación y de reserva.
- Las copias de seguridad se cifran (AES-256-CBC, PBKDF2 con 200 000 iteraciones) antes de salir del servidor y solo viajan por conexiones cifradas. No se escribe ningún archivo sin cifrar.

2. Protección en el navegador

- Content-Security-Policy: los scripts en línea solo se ejecutan si están aprobados mediante un hash SHA-256 por script o mediante un nonce por solicitud en unas pocas páginas dinámicas (sin unsafe-inline para scripts — los estilos en línea siguen permitidos; object-src 'none', base-uri 'self', frame-ancestors 'none' salvo en las páginas LTI, que solo pueden incrustar las plataformas de aprendizaje registradas). Se recogen los informes de infracciones, con limitación de frecuencia. Las páginas pensadas para niños no cargan scripts de terceros. En las páginas para adultos, los únicos scripts de terceros son Google Analytics, tras el consentimiento, y la verificación Cloudflare Turnstile en los formularios de acceso y de registro.
- Las fuentes web se alojan en el propio servidor del Encargado. No se envía ninguna solicitud a Google Fonts ni a ningún otro proveedor de fuentes.
- Cabeceras de seguridad: X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy y Cross-Origin-Resource-Policy same-origin. Se eliminan las cabeceras de versión del servidor y de PHP. Se rechazan HTTP TRACE y TRACK.
- Cookies: la cookie de sesión es Secure, HttpOnly y SameSite=Strict, con modo de sesión estricto; el identificador de sesión cambia al iniciar sesión, al activar un código y cada 30 minutos. La cookie «recordarme» está firmada con HMAC con una clave del servidor. La cookie de estado LTI se limita a /lti/ y está particionada.
- El service worker de los juegos nunca almacena en caché respuestas marcadas como no-store o private, ni ninguna ruta reservada a miembros, de modo que no queda contenido de miembros en la caché de un dispositivo compartido tras cerrar sesión.
- Las respuestas que contienen datos personales o contenido reservado a miembros se envían con Cache-Control: private, no-store, y la red de distribución de contenidos nunca las almacena en caché.

3. Control de acceso y autenticación

- Cuentas nominativas de docentes: un código de centro se usa una sola vez, para darse de alta. Crea una cuenta nominativa con una dirección de correo verificada o vincula el centro a la cuenta que el docente ya tiene. Después, el docente accede con su propio correo y contraseña, o mediante inicio de sesión

único. Un dispositivo que solo ha introducido un código de centro puede jugar, pero no tiene herramientas docentes. Un código de administración solo da de alta la primera cuenta de administración del centro y queda agotado cuando esa cuenta se confirma; a partir de entonces, el profesorado se une con un código de personal que un administrador del centro crea en el Servicio, que se muestra una sola vez, se guarda solo como hash con clave y puede sustituirse en cualquier momento.

- Las contraseñas de los docentes se guardan con hash bcrypty se comparan en tiempo constante. La dirección de correo electrónico debe verificarse antes del primer inicio de sesión. Cambiar la contraseña cierra todas las sesiones. Un administrador del centro puede retirar de inmediato el acceso de un docente.
- La verificación en dos pasos (TOTP, con códigos de respaldo en hash) es obligatoria para los administradores del centro y para los superadministradores del Encargado, y cualquier docente o coordinador de una licencia de empresa u hotel puede activarla. El código QR de alta se genera en el servidor, de modo que el secreto nunca sale de él. El segundo factor se comprueba antes de crear cualquier sesión, y los administradores del centro deben usarlo allí donde se ven datos del alumnado. La persona de contacto de protección de la infancia también debe usarlo para leer los avisos de protección. Tras 10 códigos erróneos en 24 horas, el segundo factor de la cuenta se bloquea durante 15 minutos y se avisa por correo electrónico al titular de la cuenta.
- Los códigos de acceso se guardan solo como hashes con clave en un archivo fuera de la raíz web; la clave se guarda fuera de la raíz web. Los códigos de registro y de licencia se guardan del mismo modo; un código se muestra una sola vez, cuando se crea.
- Limitación de frecuencia en el inicio de sesión (por dirección IP y por par correo electrónico/IP, con un tope global), el registro, el canje de códigos, la incorporación a clases, la incorporación a cuestionarios en directo, la sincronización del progreso, el formulario de presupuesto, los inicios de sesión LTI, los puntos de telemetría y las consultas de retorno de Stripe. Tokens CSRF en todo formulario que modifique datos. Protección contra redirecciones abiertas en todo parámetro next=.
- Derechos de acceso comprobados en el servidor: los recursos reservados a miembros (vídeos de las misiones, bancos de preguntas del trivial, libros, contenido LTI) solo se entregan tras comprobar en el servidor una sesión de código válida, un código recordado firmado o una cuenta con sesión iniciada. Nada de lo que el navegador escriba por sí mismo concede acceso.
- Aislamiento por roles y por centro: cada docente ve solo sus propias clases; los administradores del centro ven todas las clases de su propio centro y nada de otros centros; los docentes que acceden por LTI ven solo las clases del curso desde el que accedieron; el acceso de superadministrador se limita al personal identificado del Encargado.
- Todas las consultas a la base de datos utilizan sentencias preparadas; sin exec, eval ni unserialize; las rutas de archivo se construyen solo a partir de elementos de una lista permitida; las cargas (archivos CSV/ZIP de listas de clase, imágenes de encuestas) tienen tamaño limitado, se comprueba su tipo y se guardan fuera de la raíz web; la visualización de errores de PHP está desactivada.
- Inicio de sesión único opcional para el personal de empresas y hoteles mediante OpenID Connect (Authorization Code con PKCE; tokens de identidad firmados y verificados en emisor, audiencia, caducidad y nonce). Los secretos de cliente se guardan cifrados. Las cuentas solo se asocian dentro de los dominios de correo autorizados del Responsable y nunca se vinculan a una cuenta de otra organización.

4. Minimización de datos y datos de menores

- No se recogen direcciones de correo electrónico, apellidos, fotografías, fechas de nacimiento, direcciones postales, ubicaciones ni identificadores del dispositivo o publicitarios del alumnado. Las importaciones de listas conservan el nombre de pila y, como máximo, las 3 primeras letras del apellido. El alumnado por LTI se guarda con un hash con clave del identificador de usuario de la plataforma, con nombre de pila e inicial; el Responsable configura su plataforma para que comparta solo el nombre.
- Las direcciones IP se guardan solo como hashes con clave (prefijo). Quien tenga la clave podría volver a vincularlas, por lo que están seudonimizadas, no anonimizadas. Cuando acompañan a un contenido, se eliminan a los 30 días.
- Las páginas pensadas para niños (/game, /games, /trivia, /library, /sdg, /wordle, /missions, /books y sus versiones en otros idiomas) no cargan analítica ni muestran banner de consentimiento. En las demás páginas, la analítica solo se carga tras el consentimiento expreso.
- Los vídeos de las misiones para miembros los aloja el Encargado y se sirven tras la comprobación de derechos de acceso. Donde queda un reproductor de YouTube (juego libre), utiliza youtube-nocookie.com y solo se carga cuando el usuario pulsa reproducir.
- Publicar en la clasificación pública del trivial es voluntario después de cada partida, con un apodo generado (un adjetivo y un animal; sin texto libre ni nombre de centro). La clasificación pública muestra apodo y puntuación de los 10 mejores de los últimos 30 días, y las entradas se suprimen a los 30 días. Cada fila pública tiene un enlace para denunciarla; una fila denunciada tres veces se oculta hasta su revisión. Las clasificaciones de clase solo las ven el docente de esa clase y los administradores del centro, que pueden retirar filas.
- Las respuestas de texto libre se filtran automáticamente al enviarse: se eliminan las direcciones de correo electrónico y los números de teléfono, y las respuestas que coinciden con una breve lista de palabras que pueden indicar que un menor está en riesgo se retiran de los datos del estudio y se trasladan solo a la persona de contacto para la protección de la infancia designada por el centro. Los nombres no se eliminan automáticamente; los investigadores que leen las respuestas marcan los posibles nombres y nunca los incluyen en ningún informe. Una posible revelación se traslada a la persona de contacto designada por el centro en un plazo de un día lectivo. Si no se ha designado un contacto de protección de la infancia, los destinatarios previstos en la cláusula 4.4 ocupan su lugar.
- Las direcciones de correo electrónico de madres y padres en el procedimiento de consentimiento nunca se guardan en claro; solo se conserva un hash con clave.
- Los informes de la organización son agregados: una cifra basada en menos de 5 familias se oculta dentro del propio cálculo, de modo que ni la pantalla ni el CSV pueden mostrarla. Solo los administradores de la organización, con inicio de sesión en dos pasos, pueden abrirlos; cada consulta y cada exportación tienen un límite de frecuencia y quedan registradas.

5. Disponibilidad, copias de seguridad y recuperación

- Lo siguiente se ejecuta automáticamente. Un monitor independiente (UptimeRobot, 11 monitores, cada 5 minutos) avisa al Encargado si algo falla.
- Una copia de seguridad cifrada cada noche de la base de datos y de la aplicación; una copia se guarda en un centro de datos independiente en otro país de la UE. Cada mes se prueba automáticamente una restauración.
- Una copia de seguridad antes de cada versión, con un procedimiento de vuelta atrás probado; se conserva la versión de producción anterior.
- Un servidor de reserva mantiene una copia de la aplicación y una réplica en directo de la base de datos. Si falla el servidor web principal, un balanceo de carga con comprobaciones de estado desvía el tráfico

automáticamente; si falla el servidor de base de datos, la réplica se promueve mediante un procedimiento automatizado y ensayado. Ambos se probaron en octubre de 2026.

- Una comprobación horaria de la infraestructura (estado y retraso de la réplica, caducidad de certificados, espacio en disco, actualizaciones de seguridad pendientes, rangos de direcciones de la red de distribución de contenidos). Las actualizaciones de seguridad del sistema operativo se instalan automáticamente. Protección contra DDoS y bots en el perímetro de la red.
- El entorno de pruebas está separado de producción (usuario Unix distinto, pool de PHP con open_basedir, instancia de base de datos distinta, secretos eliminados).

6. Registro y supervisión

- Los eventos de seguridad (inicios de sesión fallidos, canjes de códigos, acciones administrativas, informes de infracciones de CSP, supresiones y depuraciones por conservación) se registran con hashes con clave de las direcciones IP. El registro de auditoría de seguridad se conserva 12 meses y los registros de limitación de frecuencia 30 días (anexo I, sección C).
- El estado del servicio en directo y cada incidencia se publican en la página pública de estado.

7. Medidas organizativas

- El acceso a los sistemas de producción se limita a personas identificadas. Toda cuenta administrativa (alojamiento, servidores de base de datos y de copias de seguridad, red de distribución de contenidos y DNS, repositorio de código fuente, supervisión, correo electrónico) utiliza autenticación de dos factores. El acceso a los servidores se realiza con claves SSH. Los cortafuegos limitan el acceso a la base de datos y al servidor de reserva a los equipos propios del Encargado y a los rangos de direcciones de la red de distribución de contenidos.
- Los cambios se prueban automáticamente (integración continua; una versión se rechaza si el código no la supera), pasan primero por el entorno de pruebas y se comprueban en directo tras cada versión (47 comprobaciones en directo). Se realiza y documenta una revisión estática de seguridad de la aplicación (la última, el 16 de octubre de 2026).
- Prueba de penetración, octubre de 2026: una prueba estructurada de caja blanca y caja gris de la plataforma (autenticación, sesiones, control de acceso entre centros, pagos, exposición de archivos y datos, limitación de intentos y caché perimetral), realizada por el propio equipo de pruebas del Encargado. Todos los hallazgos críticos, altos y medios se corrigieron y se volvieron a probar antes de la publicación. Está prevista una prueba de penetración externa a cargo de una empresa independiente.
- Se publica un canal de comunicación de vulnerabilidades en /.well-known/security.txt. Se acusa recibo de las comunicaciones en un plazo de 5 días hábiles y los problemas críticos se corrigen antes que cualquier otro trabajo.
- Un procedimiento escrito de gestión de incidentes establece cómo el Encargado detecta, contiene y registra una violación de la seguridad de los datos personales y cómo cumple el plazo de notificación de 48 horas de la cláusula 9.
- El Encargado lleva un registro de los tratamientos que efectúa por cuenta de responsables (artículo 30.2 del RGPD) y una evaluación de la transferencia para cada Subencargado situado fuera del EEE.
- Los plazos de conservación se definen en el código que los aplica, de modo que el plazo publicado y el plazo aplicado no pueden divergir.
- Los secretos (clave restringida de Stripe, credenciales de acceso único, claves de hash) se guardan fuera de la raíz web y nunca se incluyen en el repositorio de código fuente.

Anexo III — Subencargados y servicios de terceros

El Centro de confianza (https://eco-heroes.org/trust/#subprocessors) muestra las mismas dos listas.

Parte A — Subencargados que tratan Datos del Responsable

Anexo III.A — subencargados autorizados

Subencargado	Qué hace	Dónde	Garantía para la transferencia
Internet Girona, sobre infraestructura de OVHcloud	Alojamiento web	Francia (UE)	Dentro de la UE; condiciones estándar de tratamiento de datos del proveedor
Hetzner Online GmbH, Gunzenhausen, Alemania	Alojamiento de la base de datos, servidor de reserva y copias de seguridad cifradas	Alemania y Finlandia (UE)	Dentro de la UE; condiciones estándar de tratamiento de datos de Hetzner
Cloudflare, Inc., San Francisco, EE. UU.	Distribución de contenidos, TLS, protección contra ataques y bots, la verificación Turnstile en los formularios de acceso y de registro, y conmutación automática en caso de fallo	Red perimetral mundial; servidores de origen en la UE	Condiciones estándar de tratamiento de datos de Cloudflare con las cláusulas contractuales tipo (2021/914); Marco de Privacidad de Datos UE-EE. UU. cuando Cloudflare figure en la lista
Proton AG, Ginebra, Suiza	Alojamiento del correo electrónico de info@ y security@eco-heroes.org: correspondencia de soporte y de protección de datos con el personal del Responsable	Suiza	Decisión de adecuación de la Comisión Europea para Suiza; condiciones estándar de tratamiento de datos de Proton
Google (Google Ireland Ltd / Google LLC) — solo acceso e importación de Classroom	Solo si el Responsable los activa: acceso de docentes (nombre, dirección de correo electrónico, identificador; sin datos del alumnado); importación de listas de Google Classroom (nombre y apellido leídos una vez y guardados como nombre de pila más inicial; el token de acceso permanece en la sesión del docente)	UE / EE. UU.	Condiciones de Google del propio Responsable; condiciones estándar de tratamiento de datos de Google con las cláusulas contractuales tipo; Marco de Privacidad de Datos UE-EE. UU. cuando figure en la lista
Microsoft (Microsoft Ireland Operations Ltd) — solo acceso	Solo si el Responsable lo activa: acceso de docentes (solo identidad; sin datos del alumnado)	UE / EE. UU.	Condiciones de Microsoft del propio Responsable; DPA de productos y servicios de Microsoft con las cláusulas contractuales tipo; Marco de Privacidad de Datos UE-EE. UU. cuando figure en la lista

Subencargado	Qué hace	Dónde	Garantía para la transferencia
Google (YouTube, youtube-nocookie.com)	Reproducción de vídeos educativos seleccionados donde aún se usa un reproductor de YouTube: modo de privacidad mejorada, cargado solo cuando el usuario pulsa reproducir	UE / EE. UU.	Condiciones de Google; Marco de Privacidad de Datos UE-EE. UU. cuando figure en la lista
Moodle Pty Ltd (MoodleCloud), Australia Occidental	Solo si el Responsable utiliza el sitio de cursos de Eco Heroes eco-heroes.moodlecloud.com en lugar de su propia plataforma de aprendizaje: cuentas de curso en ese sitio y el progreso que los juegos le comunican	Alojamiento de MoodleCloud en Amazon Web Services	Acuerdo de tratamiento de datos de MoodleCloud con las cláusulas contractuales tipo (2021/914) para toda transferencia fuera del EEE

Parte B — Servicios de terceros que no tratan Datos del Responsable

Se enumeran por transparencia. Cuando hay datos personales, se aplica la Política de privacidad del Encargado. El propio servidor de correo del Encargado envía los correos de cuenta, de verificación y de servicio; no es un tercero.

Anexo III.B — servicios de terceros fuera de este Acuerdo

Servicio	Qué hace	Dónde	Por qué queda fuera de este Acuerdo
Stripe	Pagos con tarjeta de las suscripciones familiares en el sitio web; el Encargado consulta el estado del pago y de la suscripción	UE / EE. UU.; condiciones de tratamiento de datos de Stripe con las cláusulas contractuales tipo; Marco de Privacidad de Datos UE-EE. UU.	Los suscriptores familiares son clientes propios del Encargado; no se envían datos del centro a Stripe
Google Analytics 4	Estadísticas de visitas en páginas públicas para adultos, solo tras el consentimiento; nunca en las páginas pensadas para niños ni en el área docente	UE / EE. UU.; condiciones de tratamiento de datos de Google con las cláusulas contractuales tipo; Marco de Privacidad de Datos UE-EE. UU.	No se envía ningún Dato del Responsable; el Encargado es responsable de sus propias estadísticas web
Formspree	Entrega los mensajes enviados con el formulario de contacto general	EE. UU.; condiciones estándar de tratamiento de datos del proveedor (cláusulas contractuales tipo; Marco de Privacidad de Datos UE-EE. UU. cuando figure en la lista)	Los mensajes son correspondencia propia del Encargado; el Servicio no lo utiliza
Brevo	Correos de Dinner Questions para familias (con suscripción; solo la dirección de correo electrónico)	UE	Boletín para familias; el Servicio no lo utiliza
RevenueCat	Estado de la suscripción en la aplicación (solo identificador de cuenta e historial de compras)	EE. UU.; cláusulas contractuales tipo	Cuentas familiares de la aplicación; sin datos del centro

Servicio	Qué hace	Dónde	Por qué queda fuera de este Acuerdo
Google Play / Apple App Store	Pagos de suscripción dentro de la aplicación, cobrados por la tienda	UE / EE. UU.	Las tiendas venden la suscripción como responsables independientes
Google / Apple (acceso en la aplicación)	Acceso opcional de madres y padres en la aplicación (dirección de correo electrónico e identificador de acceso)	UE / EE. UU.; Marco de Privacidad de Datos UE-EE. UU., cláusulas contractuales tipo	Cuentas familiares de la aplicación; sin datos del centro
UptimeRobot	Comprueba que las páginas públicas y el punto de estado responden	UE / EE. UU.	No trata datos personales

Anexo IV — Datos de menores

Este anexo completa los anexos I y II para el alumnado menor de 18 años.

1. **Edad de consentimiento digital.** Cuando la ley aplicable al Responsable exija el consentimiento para servicios de la sociedad de la información ofrecidos directamente a un niño (artículo 8 del RGPD), el Responsable lo obtiene y lo registra. La edad es de 14 años en España (artículo 7 de la LOPDGDD), de entre 13 y 16 años en los demás Estados miembros de la UE y de 13 años en el Reino Unido; para los centros de los Estados Unidos, véase el anexo V. Cuando el Responsable se base en otra base jurídica para el uso escolar, como el cumplimiento de una misión realizada en interés público, no se necesita consentimiento y el Responsable informa al alumnado y a las familias. El Servicio no comprueba la edad. Sus dos franjas de edad (9-12 y 13-17) solo eligen el contenido y la versión de los vídeos.
2. **Procedimiento de consentimiento parental en el sitio web.** Cuando una función del sitio web necesita el consentimiento de un progenitor para un niño que no ha alcanzado la edad de consentimiento digital, el Servicio no registra nada hasta que el progenitor confirma mediante un enlace de un solo uso enviado por correo electrónico. Solo se guardan un hash con clave de la dirección de correo electrónico del progenitor, la decisión y las marcas de tiempo. Las solicitudes sin respuesta se suprimen a los 30 días y las denegaciones a los 12 meses. Retirar el consentimiento borra los datos recogidos con él.
3. **Plan familiar.** La suscripción familiar la contrata una madre, un padre o un tutor, que es cliente del Encargado. En el sitio web, el proceso de pago pide al comprador que confirme que es mayor de edad; en la aplicación, los pasos de acceso y de compra están detrás de una comprobación para adultos (una pregunta aritmética escrita). Ninguna de las dos es una verificación de identidad o de edad. Los niños no abren cuentas en el sitio web. Un niño puede utilizar un código familiar bajo la responsabilidad de su progenitor; no se le asocian datos del centro.
4. **Sin perfiles y sin publicidad.** El Encargado no muestra publicidad ni utiliza identificadores o SDK publicitarios. No elabora perfiles del alumnado más allá de la vista de progreso que ven los docentes del Responsable, no toma decisiones automatizadas con efectos jurídicos o similarmente significativos y nunca vende ni comparte datos del alumnado con fines publicitarios.
5. **Sin analítica en las páginas para niños.** Las páginas pensadas para niños (el juego de aventuras, el centro de juegos, el trivial, la biblioteca, las páginas de los objetivos, Wordle, las misiones y los libros, en los 13 idiomas) no cargan analítica, seguimiento ni banner de consentimiento. Solo utilizan el almacenamiento del navegador estrictamente necesario (idioma, progreso en el dispositivo, sesión).
6. **Estudios de impacto.** Cuando el Responsable inscribe clases en un estudio de impacto, el alumnado responde en clase como parte de la evaluación que el propio Responsable hace de su enseñanza. El Responsable informa a las familias con antelación y ofrece la posibilidad de exclusión, o recoge el consentimiento por escrito cuando su ley o su normativa lo exijan; el Servicio admite ambas opciones y excluye las plazas afectadas. El alumnado puede omitir cualquier pregunta y se le indica en la primera pantalla. Los docentes solo ven resultados de clase, y solo cuando al menos 10 alumnos han respondido antes y después; ningún usuario del centro ve las respuestas individuales de un alumno. Una respuesta de texto libre que pueda contener una revelación relevante para la protección de la infancia se traslada al contacto de protección de la infancia designado por el Responsable, que decide qué hacer. El Encargado solo utiliza resultados agregados y anonimizados conforme a la cláusula 2.3, nunca texto libre. Una posible revelación se traslada a la persona de contacto designada en un plazo de un día lectivo, y solo esa persona la ve. Si no se ha designado un contacto de protección de la infancia, los destinatarios previstos en la cláusula 4.4 ocupan su lugar.

7. **Sin funciones de comunicación.** El Servicio no tiene chat, mensajería ni perfiles públicos del alumnado. La clasificación pública del trivial es voluntaria, utiliza solo apodos elegidos de una lista generada, no muestra el nombre del centro, conserva las entradas 30 días y tiene un enlace de denuncia en cada entrada. Las clasificaciones de clase solo las ven el docente de la clase y los administradores del centro, y una entrada pública denunciada tres veces se oculta hasta su revisión.
8. **Riesgo residual comunicado al Responsable.** Un compañero que conozca un código de clase y el apodo de un alumno puede abrir el progreso de ese alumno en otro dispositivo. Los docentes pueden ver, renombrar o eliminar alumnos en cualquier momento y pueden renovar el código de clase. El Responsable lo tiene en cuenta en su propia evaluación y en la forma de repartir los códigos de clase.
9. **Derechos del alumnado y de las familias.** Las familias y el alumnado ejercen sus derechos ante el Responsable. Los docentes del Responsable pueden consultar, exportar, renombrar, restablecer y eliminar directamente los datos de un alumno. El Encargado remite al Responsable cualquier solicitud que reciba (cláusula 8.2).
10. **Información para los niños.** El Encargado publica un Aviso de privacidad infantil con una parte escrita para los niños (parte A) y una parte para familias y centros (parte B) en https://eco-heroes.org/legal/children/. El Responsable puede reutilizarlo en su propia información al alumnado y a las familias.

Anexo V — Responsables en el Reino Unido y en los Estados Unidos

1. **Reino Unido.** Cuando el Responsable esté establecido en el Reino Unido, las referencias de este Acuerdo al RGPD se entienden hechas al UK GDPR y a la Data Protection Act 2018, y la autoridad de control competente es la Information Commissioner's Office (ICO). Los Datos del Responsable pasan del Reino Unido al EEE en virtud de la normativa de adecuación del Reino Unido para el EEE. Las transferencias ulteriores a los Estados Unidos se basan en la extensión del Reino Unido al Marco de Privacidad de Datos UE-EE. UU. cuando el proveedor esté certificado, o en la adenda del Reino Unido de transferencia internacional de datos (UK International Data Transfer Addendum) a las cláusulas contractuales tipo. El Encargado diseña el Servicio teniendo en cuenta el Age Appropriate Design Code de la ICO; su resumen de conformidad figura en la sección 11 de la Política de privacidad.
2. **Estados Unidos — FERPA.** Cuando el Responsable sea un centro o distrito escolar de los Estados Unidos sujeto a la Family Educational Rights and Privacy Act, el Encargado actúa como «school official» con un interés educativo legítimo conforme a 34 CFR 99.31(a)(1)(i)(B). El Encargado está bajo el control directo del Responsable en cuanto al uso y la conservación de los expedientes educativos, los utiliza solo para los fines de la Licencia y no los comunica a nadie más, salvo a los Subencargados conforme a la cláusula 6 o cuando la ley lo exija.
3. **Estados Unidos — COPPA.** Para el alumnado menor de 13 años, el Responsable puede consentir en nombre de las familias la recogida de los datos descritos en el anexo I, como permiten las orientaciones de la Federal Trade Commission, porque los datos se utilizan solo para los fines educativos del Responsable y para ningún otro fin comercial. El Responsable mantiene informadas a las familias y transmite sus solicitudes de revisar o suprimir los datos de su hijo; el Encargado las atiende conforme a la cláusula 8.
4. **Estados Unidos — supresión y notificación.** La cláusula 10 se aplica a la supresión al fin de la Licencia. Cuando una ley estatal sobre privacidad del alumnado fije un plazo más breve para la notificación de violaciones o la supresión, el Encargado lo cumple en cuanto el Responsable le indique qué ley se aplica.