GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació

DGIE

aepd agencia española protección datos

Apps edu

Buenas Prácticas Educativas en Privacidad y Protección de Datos Personales para un Uso Responsable y Seguro de Internet para los Menores

Conselleria de Educación, Cultrua, Universidades y Empleo
Dirección General de Infraestructuras Educativas
Av. de Campanar, 32
Valencia 46015
Telf. 961970200
dgiedu@gva.es

Octubre 2024

ÍNDICE

1. Introducción

La Dirección General de Infraestructuras Educativas de la Conselleria de Educación, Cultura, Universidades y Empleo de la Generalitat Valenciana se complace en presentar la candidatura a los **Premios de la Agencia Española de Protección de Datos** a **las Buenas Prácticas Educativas en Privacidad y Protección de Datos Personales para un Uso Responsable y Seguro de Internet para los Menores** el proyecto Appsedu**,** mediante la aportación de la memoria descriptiva del proyecto.

Appsedu es una **plataforma innovadora destinada a ofrecer un catálogo exhaustivo de aplicaciones educativas verificadas y seguras para el entorno escolar.** Les invitamos a acceder al portal de Appsedu a través del siguiente enlace:

https://portal.edu.gva.es/appsedu/es/inicio/

La Conselleria de Educación, Cultura, Universidades y Empleo tiene la competencia para decidir qué aplicaciones se autorizan para su uso en los centros educativos. La puesta en marcha de Appsedu permite a la Conselleria de Educación, Cultura, Universidades y Empleo junto con la comunidad educativa cumplir con la legislación vigente en cuanto a protección de datos y ciberseguridad.

Resulta esencial cumplir con diversas normativas tanto a nivel europeo como estatal y autonómico en el desarrollo y funcionamiento de Appsedu, especialmente en lo que respecta a la protección de datos y la seguridad de la información. Las normativas relevantes incluyen:

Normativa Europea y Estatal:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, conocido como el Reglamento General de Protección de Datos (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 2/2006, de 3 de mayo, de Educación.

Normativa Autonómica:

- Resolución de 28 de junio de 2018, de la Subsecretaría de la Conselleria de Educación, Investigación, Cultura y Deporte, por la que se dictan instrucciones para el cumplimiento de la normativa de protección de datos en los centros educativos públicos de titularidad de la Generalitat.

Además, cada curso escolar se emiten las Instrucciones de Inicio de Curso, las cuales proporcionan una concreción de las normativas anteriores en el contexto específico del curso escolar.

Este proyecto representa un **avance significativo en el ámbito de la tecnología educativa** al abordar de manera integral los desafíos relacionados con la ciberseguridad y la protección de datos en el uso de aplicaciones en el ámbito educativo.

1.1. Finalidad de Appsedu

Appsedu tiene como **finalidad** proporcionar a la comunidad educativa un **recurso confiable y seguro para acceder a aplicaciones** que cumplan con los más altos estándares de seguridad y protección de datos.

Este catálogo de aplicaciones abarca una amplia gama de plataformas, desde ordenadores con distintos sistemas operativos hasta dispositivos móviles y aplicaciones web, garantizando así la accesibilidad y versatilidad para todos los usuarios del entorno educativo.

Uno de los **aspectos más destacados** de Appsedu es su **capacidad para gestionar el consentimiento de los usuarios en el contexto del inicio de sesión único SSO (single sign-on en aplicaciones de terceros**. Esto se logra mediante un sistema que garantiza que los datos personales de los usuarios, especialmente aquellos relacionados con el profesorado y el alumnado, estén protegidos y se utilicen de manera ética y legal, en pleno cumplimiento de las normativas vigentes, incluido el RGPD y la legislación nacional y autonómica aplicable.

1.2. Colaboraciones

El desarrollo de Appsedu no está exento de **desafíos** especialmente en lo que respecta a **garantizar la seguridad y la protección de datos en un entorno educativo digital** cada vez más complejo y dinámico.

Para abordar estos retos, se han establecido **colaboraciones estratégicas** con expertos en ciberseguridad y protección de datos, así como con distintas entidades de la Generalitat Valenciana.

En particular, se han desarrollado dos protocolos de evaluación de ciberseguridad para analizar exhaustivamente las vulnerabilidades de las aplicaciones solicitadas.

Estos protocolos, denominados protocolo básico y protocolo estándar, permiten una evaluación rigurosa y detallada de las aplicaciones, garantizando así que sólo aquellas que cumplen con los más altos estándares de seguridad sean incluidas en el catálogo de Appsedu.

La **colaboración** con la **Delegación de Protección de Datos de la Generalitat Valenciana** ha sido fundamental para garantizar el cumplimiento de las normativas de protección de datos y proporcionar asesoramiento experto en la redacción de los encargos de tratamiento de datos necesarios para las aplicaciones que requieren dicha consideración.

La **verificación de los protocolos de análisis de aplicaciones** por parte de la **Subdirección General de Ciberseguridad de la Generalitat Valenciana**, junto con el asesoramiento continuo del **CSIRT-CV**, ha fortalecido aún más la seguridad y la confiabilidad de Appsedu, convirtiéndola en una plataforma de referencia en el ámbito educativo.

2. Objetivos del proyecto

Como hemos mencionado en el punto 1.1. la **finalidad** del proyecto es proporcionar a la comunidad educativa un **recurso confiable y seguro para acceder a aplicaciones** que cumplan con los más altos estándares de seguridad y protección de datos.

Para lograrlo hemos establecido los siguientes objetivos específicos:

1. Implementar un sistema centralizado de gestión de aplicaciones educativas que garantice la seguridad y protección de datos.

2. Establecer protocolos de evaluación rigurosos para analizar la ciberseguridad y protección de datos de las aplicaciones solicitadas por los centros educativos.

3. Proporcionar a los usuarios (profesorado y alumnado) un entorno digital seguro y eficiente para el desarrollo de actividades educativas.

4. Asegurar que se cumple la normativa de protección de datos.

Estos objetivos específicos han guiado nuestras acciones y nos han permitido alcanzar los resultados deseados.

A lo largo de este proyecto, hemos trabajado en colaboración con diferentes instituciones para cumplir con estas metas y generar un impacto positivo.

3. Descripción del proyecto

3.1. Contextualización

3.1.1. Situación Previa

Con anterioridad a la implementación del proyecto Appsedu, la gestión de aplicaciones en los centros educativos de la Comunidad Valenciana carecía de un enfoque centralizado.

Cada centro tenía la autonomía para instalar y utilizar cualquier aplicación sin un control riguroso. Esta falta de centralización suponía graves riesgos en términos de seguridad y protección de datos, ya que las aplicaciones no eran evaluadas en relación con aspectos de ciberseguridad y privacidad. Tanto el profesorado como el alumnado tenían la capacidad de utilizar estas aplicaciones sin ningún tipo de supervisión ni control por parte de la administración educativa.

La instalación de software se realizaba sin un análisis previo de ciberseguridad y protección de datos, lo que aumentaba significativamente el riesgo de utilizar aplicaciones no seguras y que no respetaban adecuadamente la privacidad de los datos personales, especialmente los de los menores.

Hay que tener en cuenta que con anterioridad a la pandemia ocasionada por el COVID-19, la falta de herramientas en la nube y de plataformas de comunicación digital dificultaba la colaboración y la enseñanza a distancia, lo que suponía un obstáculo adicional para el desarrollo de la educación en entornos virtuales.

Además, no existía una identidad digital (SSO: single sign-on) respaldada por un proveedor con un encargo de tratamiento de datos. Esta falta de encargo de tratamiento dificultaba la comprensión de los tratamientos de datos realizados por las aplicaciones que utilizaba cada centro educativo, lo que significaba que los usuarios, especialmente los menores, no podían ser plenamente conscientes de los riesgos asociados al uso de estas aplicaciones

¿Por qué se implementó el uso de los sistemas MDM (Mobile Device Management) en los centros públicos educativos de la Comunidad Valenciana?

Ante la situación mencionada, se hizo evidente la necesidad de implementar soluciones más efectivas que permitieran garantizar un entorno educativo seguro y protegido para todos los usuarios, tanto el profesorado como el alumnado.

Es en este contexto donde surge la iniciativa de implementar los sistemas MDM como una medida clave para mejorar la gestión de aplicaciones en los dispositivos TIC de los centros educativos.

Tras la implementación de los sistemas MDM (Mobile Device Management), gestionados de forma centralizada en la infraestructura de la Conselleria de Educación, Cultura, Universidades y Empleo y utilizados por los centros educativos, se ha logrado proporcionar un mayor control y seguridad en la gestión de las aplicaciones utilizadas en los dispositivos TIC.

Estos sistemas, como Intune para dispositivos con Windows, MacOS e iOS, ZeroCenter para sistemas Linux (distribución LliureX), Sophos para tabletas Android y Radix para pizarras digitales interactivas con Android, permiten a la Conselleria de Educación, Cultura, Universidades y Empleo tener un control centralizado sobre las aplicaciones instaladas en los dispositivos de los centros educativos.

Sin embargo, esta transición no ha estado exenta de problemas. En un principio, los centros educativos se encontraron con la situación de que no podían continuar instalando el software al que estaban habituados, ya que las tiendas de aplicaciones generadas por los MDM carecían de un amplio catálogo de opciones.

Es entonces cuando surge la necesidad de poblar las tiendas de aplicaciones con software educativo confiable, garantizando que cumpliera con los estándares de seguridad y protección de datos necesarios, especialmente teniendo en cuenta que gran parte de este software estaba destinado a ser utilizado por menores.

Este desafío impulsó la búsqueda de soluciones para garantizar la disponibilidad de un catálogo adecuado de aplicaciones educativas.

3.2. Alcance de la solución propuesta

El alcance del proyecto aborda de manera integral la gestión de aplicaciones educativas, desde la evaluación inicial hasta la gestión de accesos y el seguimiento continuo, garantizando así un entorno digital seguro y eficiente para la comunidad educativa.

A continuación, enumeramos las acciones realizadas para el desarrollo del proyecto:

1. **Implementación de MDM (Mobile Device Management):** Se ha desplegado un sistema centralizado de gestión de dispositivos móviles para controlar y administrar las aplicaciones instaladas en los dispositivos tecnológicos de los centros educativos. Esto permite una gestión eficiente de los recursos, asegurando que solo las aplicaciones autorizadas estén disponibles para su uso.

2. **Control de Acceso mediante SSO (Single Sign-On):** Se establece un sistema de inicio de sesión único que permite a los usuarios acceder de manera segura a las aplicaciones educativas utilizando sus identidades digitales gestionadas en un Tenant de Microsoft. Este mecanismo garantiza un acceso simplificado y seguro a las aplicaciones, reduciendo la carga administrativa y mejorando la experiencia del usuario.

3. **Evaluación de Aplicaciones de Terceros:** Se implementan procedimientos detallados para la evaluación de aplicaciones de terceros, tanto las que utilizan autenticación por SSO, como aquellas que utilizan otros métodos de autenticación o que no la requieren. Se analizan criterios de seguridad, privacidad y funcionalidad para garantizar que solo las aplicaciones que cumplen con los estándares establecidos sean autorizadas para su uso en entornos educativos.

4. **Control de Acceso basado en Grupos de Seguridad:** Se configura cada aplicación para que requiera asignación a un grupo de seguridad específico. Sólo los usuarios que pertenecen a este grupo tienen acceso a la aplicación mediante SSO, lo que garantiza un control preciso sobre quién puede utilizar cada aplicación autorizada.

3.3. Procesos Implementados:

En este proyecto, hemos implementado una serie de procesos con el objetivo de que la comunidad educativa tenga un recurso confiable y seguro para la gestión de las aplicaciones.

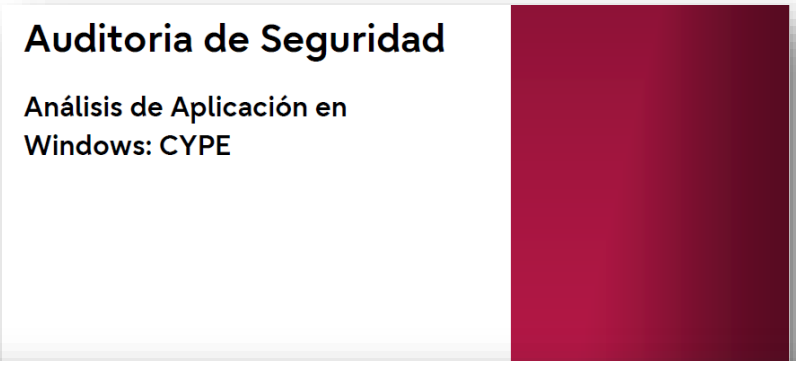
A continuación, detallamos los principales procesos que hemos puesto en marcha:

1. **Solicitud y Evaluación de Aplicaciones:** Se establece un proceso estructurado para la solicitud y evaluación de nuevas aplicaciones educativas. Las solicitudes son sometidas a un análisis exhaustivo de ciberseguridad, protección de datos y pertinencia pedagógica antes de su autorización.

2. **Gestión Automatizada de Accesos:** Se implementan mecanismos automáticos para la gestión de accesos a las aplicaciones autorizadas. Los usuarios que otorgan su consentimiento para el uso de una aplicación son automáticamente asignados a un grupo de seguridad correspondiente, y su acceso se retira automáticamente si retiran su consentimiento.

Cada uno de estos procesos es esencial para alcanzar los resultados deseados y garantizar el éxito del proyecto.

3.3.1. Ejemplo de análisis de una aplicación



Auditoria de Aplicaciones

Contenido

3. Análisis de vulnerabilidades con JOE Sandbox

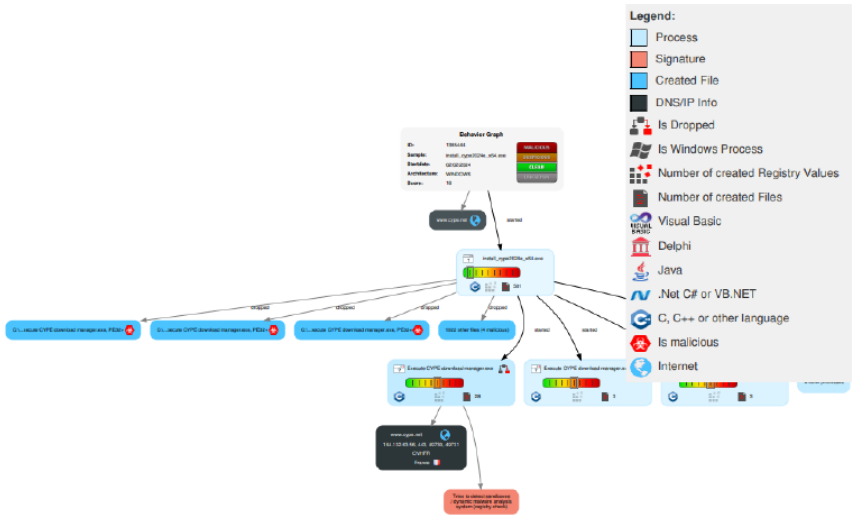
Tras realizar un análisis de Malware sobre la aplicación, se han encontrado indicios que indican que los permisos solicitados o las vulnerabilidades encontradas pueden ser maliciosas o peligrosas, por lo que la clasificación otorgada por el equipo de seguridad es **"Limpio"**

Se analiza el comportamiento de arranque:

Se analiza la posible "evasión del sistema de análisis de Malware y Sandbox" para la obtención del resultado anterior:

El programa parece detectar entornos Sandbox y sistemas de análisis antivirus.
Sería recomendable aislar el archivo en una máquina nativa preparada específicamente para ejecutar archivos sospechosos y similares.

3.1.1 Gráfico de comportamiento.



3.4. Control y seguimiento de los procesos

Desde la Dirección General de Infraestructuras Educativas se establece un sistema de seguimiento continuo para monitorear el uso de las aplicaciones autorizadas y evaluar su impacto pedagógico.

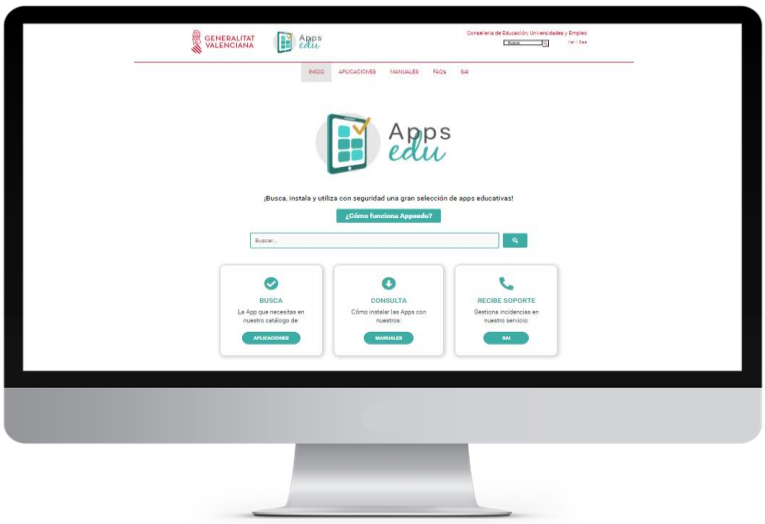
1. Realización de auditorías periódicas para garantizar el cumplimiento de los estándares de seguridad y privacidad.

2. Puesta en marcha de procedimientos de respuesta rápida para abordar cualquier irregularidad o incumplimiento por parte de las aplicaciones autorizadas, asegurando un entorno educativo seguro y protegido para todos los usuarios.

3.5. Funcionalidades de Appsedu

El conjunto de funcionalidades de Appsedu aborda diversas necesidades y garantiza un acceso controlado y transparente a un amplio catálogo de aplicaciones educativas:

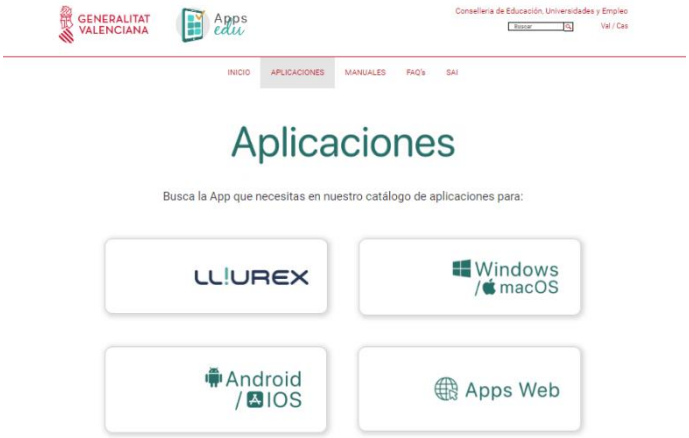
https://portal.edu.gva.es/appsedu/es/inicio/



A continuación, se detallan con mayor profundidad las principales funcionalidades de Appsedu.

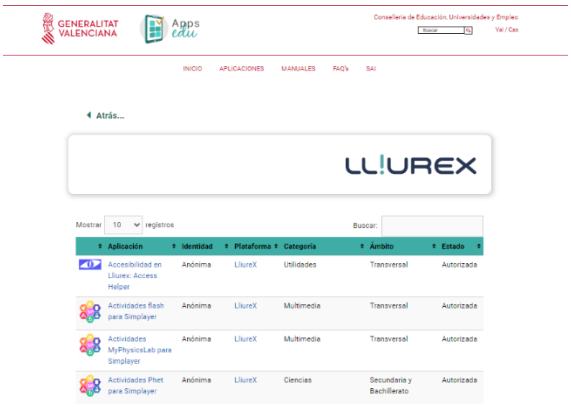
1. **Catálogo de Aplicaciones Evaluadas:**

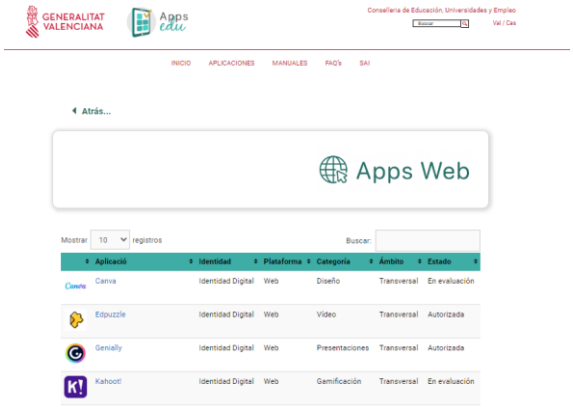
Appsedu proporciona un amplio catálogo de aplicaciones, cada una evaluada meticulosamente para garantizar su seguridad, privacidad y adecuación pedagógica. Desde herramientas de productividad hasta recursos interactivos, este catálogo ofrece una variedad de opciones para enriquecer el aprendizaje en el aula.



2. **Información Detallada de Aplicaciones:**

Cada aplicación en el catálogo de Appsedu está acompañada de una descripción detallada que abarca desde su propósito educativo hasta su estado de autorización. Los usuarios pueden acceder a información clave, como políticas de privacidad, términos de uso y recomendaciones de protección de datos, lo que les permite tomar decisiones informadas sobre su uso.





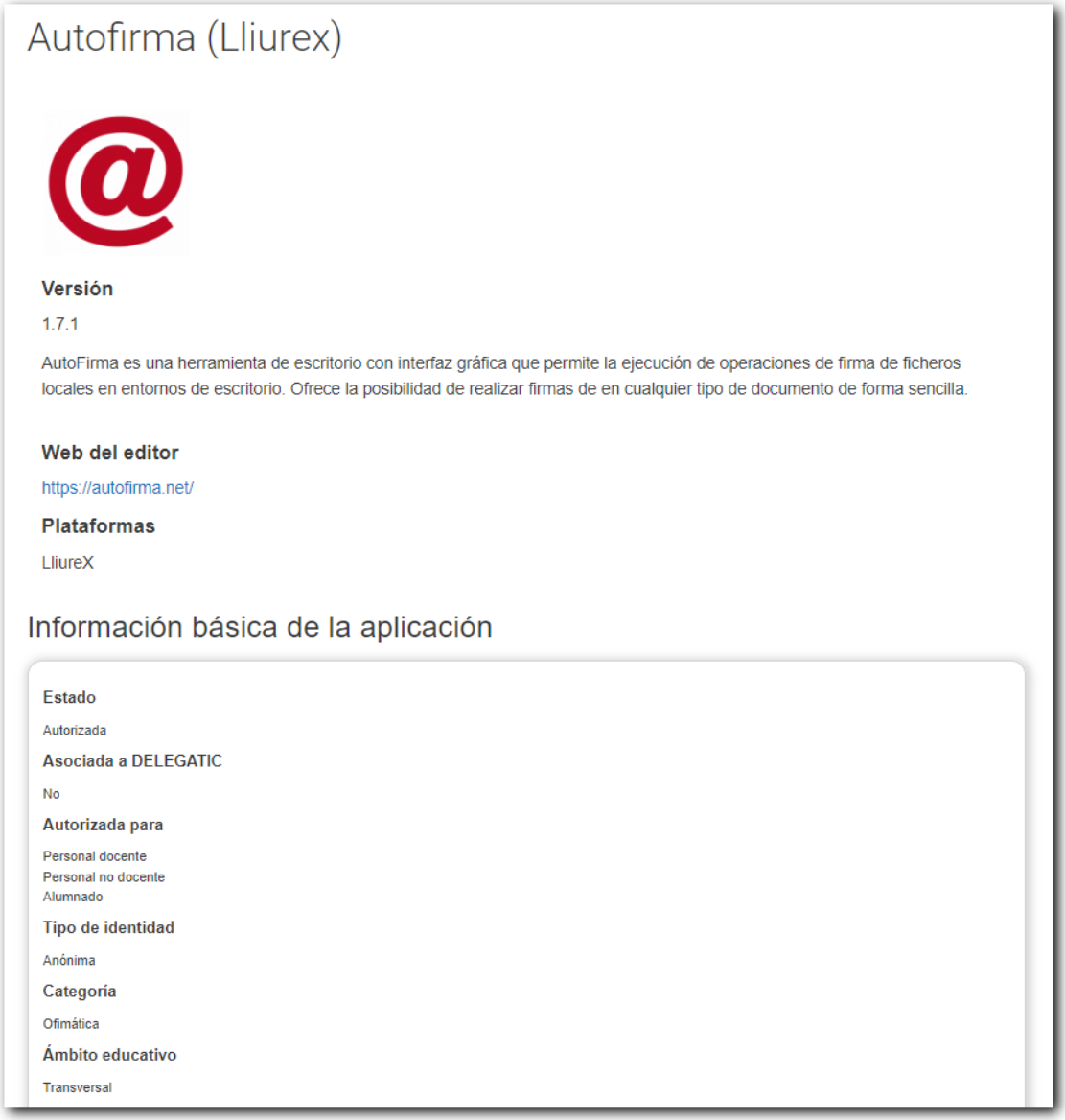
Los estados en los que se puede encontrar una aplicación son:

- Autorizada
- No autorizada
- Sin evaluar
- En evaluación
- A retirar
- Retirada

Detalle de las aplicaciones

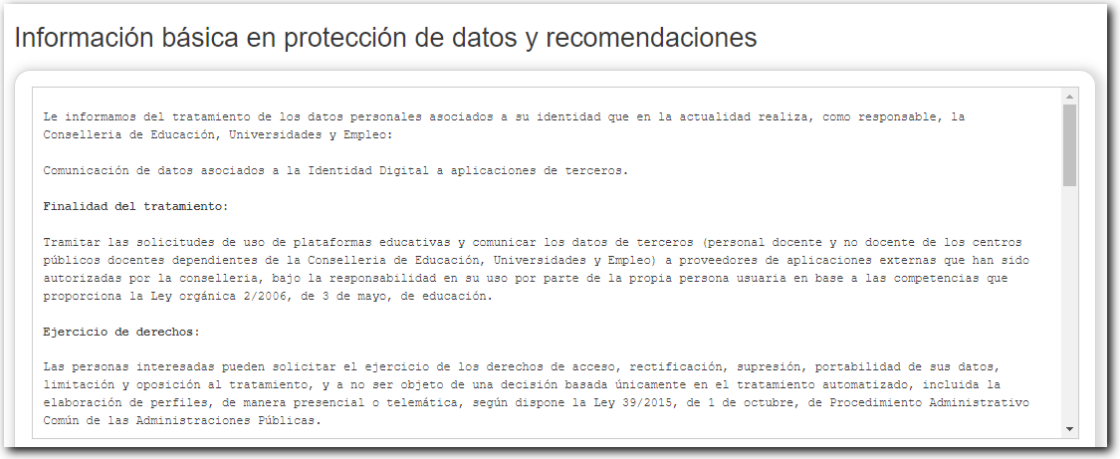
Desde las tablas anteriores se puede acceder al detalle de las aplicaciones. La información de detalle de cada aplicación que se muestra depende del tipo de aplicación y del estado de la misma.Todas las aplicaciones tienen una sección de información básica.

Véase ejemplo para la aplicación de AutoFirma.

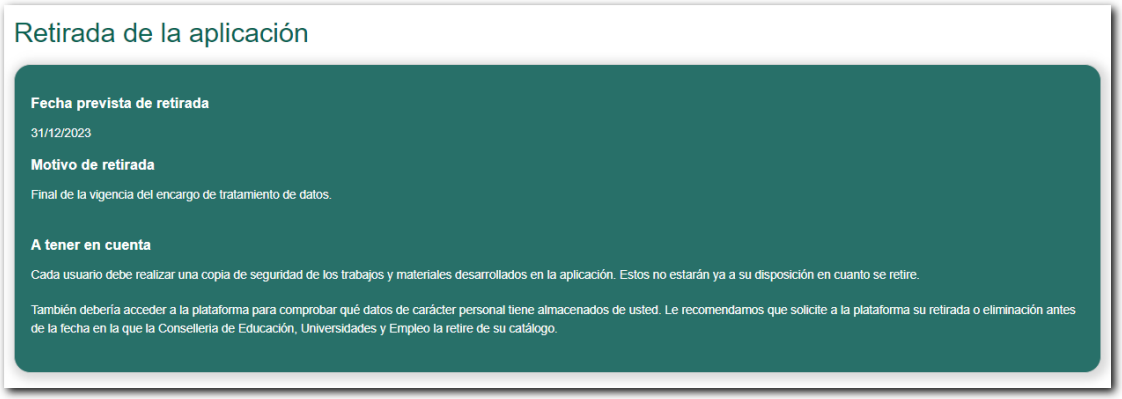


En la mayor parte de las aplicaciones hay una sección de información adicional que proporciona el editor de la aplicación.

En aquellas aplicaciones que para su acceso requieren de la recogida del consentimiento de los usuarios, se muestra información básica sobre protección de datos y recomendaciones, así como el acceso a los formularios de consentimiento y de revocación de los consentimientos.



De otro modo, en las aplicaciones que están en estado “A retirar” se advierte a los usuarios de esta situación, utilizando un color destacado. En esta situación, no se muestra el enlace al formulario para poder dar nuevos consentimientos.



3. Gestión de Consentimientos:

Los usuarios tienen la capacidad de gestionar sus consentimientos a través de Appsedu. Pueden otorgar o revocar su consentimiento para la transferencia de datos a aplicaciones de terceros según sus preferencias y necesidades, ofreciendo un control total sobre la transferencia de sus datos personales a las aplicaciones de terceros.

Formularios de Consentimiento y Revocación.

Appsedu proporciona información sobre protección de datos que se ofrece al usuario antes que este decida dar su consentimiento para la transferencia de datos a terceros. Estos formularios están diseñados permiten otorgar su consentimiento de manera transparente, informada y voluntaria.
Se generan para cada aplicación, utilizando como tecnología MS Forms. Solo los usuarios con identidad digital pueden responderlos para dar sus consentimientos. En su procesamiento se evita la recogida de consentimientos de alumnado, sólo el profesorado y el personal no docente pueden registrar sus consentimientos y revocaciones.

En los formularios se vuelve a mostrar toda la información de carácter legal en materia de protección de datos relativa al consentimiento que debe recogerse para utilizar la aplicación mediante la identidad digital.

El procesamiento de la información recogida en los formularios y las acciones sobre el Tenant se realiza mediante Power Automate.


Aplicación
Español (España, alfab...
Hola, itedu.apps. Cuando envíe este formulario, el propietario verá su nombre y dirección de correo electrónico.
Información básica en protección de datos y recomendaciones
Le informamos del tratamiento de los datos personales asociados a su identidad que en la actualidad realiza, como responsable, la Conselleria de Educación, Universidades y Empleo:
Comunicación de datos asociados a la Identidad Digital a aplicaciones de terceros.
Finalidad del tratamiento:
Tramitar las solicitudes de uso de plataformas educativas y comunicar los datos de terceros (personal docente y no docente de los centros públicos docentes dependientes de la Conselleria de Educación, Universidades y Empleo) a proveedores de aplicaciones externas que han sido autorizadas por la conselleria, bajo la responsabilidad en su uso por parte de la propia persona usuaria en base a las competencias que proporciona la Ley orgánica 2/2006, de 3 de mayo, de educación.
Ejercicio de derechos:
Las personas interesadas pueden solicitar el ejercicio de los derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición al tratamiento, y a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, de manera presencial o telemática, según dispone la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
La información completa está accesible en la siguiente página web: https://sede.gva.es/es/proc19970.
Para acceder al resto de información relativa a este tratamiento, puede pinchar en este enlace
https://ceice.gva.es/documents/161634256/169672342/17.+Comunicaci%C3%B3n+de+datos+asociados+a+la+identidad+digital+a+aplicaciones+de+terceros.pdf/5f926ca3-b343-b985-603f-582362c46e4e?t=1703073961721


Aplicación
Español (España, alfab...
* Obligatorio
Aceptación de los términos anteriores
Puede volver a la página anterior para leerlos de nuevo
Entiendo los términos anteriores y los acepto *
Sí
No
Doy mi consentimiento para que mis datos puedan ser comunicados a la aplicación:
Consentir
Quedo informado/a de la posibilidad de revocar este consentimiento en cualquier momento a través de los medios indicados en el apartado "Ejercicio de derechos"
Atrás
Enviar


Aplicación Revocación del consentimiento
9 ene 2024
Revocación del consentimiento a la transferencia de datos
Empezar ahora


Aplicación Revocación del consentimiento
Hola, itedu.apps. Cuando envíe este formulario, el propietario verá su nombre y dirección de correo electrónico.
* Obligatorio
Tras ejercer el derecho a la revocación del consentimiento a la transferencia de datos, la Conselleria de Educación, Universidades y Empleo dejará de comunicar ningún tipo de información a la aplicación Edpuzzle.
Asegúrese de haber ejercido su derecho también en la plataforma indicada. Una vez haya ejercido su derecho a de revocación del consentimiento a la transferencia de datos, dejará también de poder acceder a dicha aplicación por medio de su identidad digital
Quiero revocar el consentimiento a la transferencia de datos al tercero *
Sí
No
Enviar

4. Asignación de Grupos de Seguridad:

Se automatiza la asignación de usuarios a grupos de seguridad específicos para garantizar un acceso controlado a las aplicaciones que requieren consentimiento. Estos grupos permiten que sólo aquellos usuarios que hayan otorgado su consentimiento puedan acceder a las aplicaciones autorizadas que lo requieren, garantizando el cumplimiento del RGPD.

5. Base de Datos de Consentimientos:

Appsedu mantiene una base de datos centralizada de todos los consentimientos otorgados por los usuarios, asegurando la trazabilidad y la transparencia en el tratamiento de datos personales.

6. Notificaciones por Correo Electrónico:

La plataforma envía notificaciones por correo electrónico para informar a los usuarios sobre los consentimientos que han otorgado o revocado. Estas notificaciones garantizan que los usuarios puedan tomar decisiones informadas sobre el uso de las aplicaciones.

7. Soporte Técnico.

El profesorado puede recibir soporte para resolver cualquier incidencia o consulta relacionada con la plataforma Appsedu a través del SAI (Soporte y Asistencia Informática). Los usuarios pueden abrir tickets de soporte, recibir ayuda personalizada de los técnicos y seguir el progreso de sus solicitudes a través del sistema de tickets.

8. Guías de Uso y Preguntas Frecuentes (FAQs):

Appsedu proporciona guías detalladas de uso para ayudar a los usuarios a navegar por la plataforma y comprender los procesos de consentimiento y revocación. Estas FAQs abordan preguntas comunes y ofrecen respuestas claras y concisas para una experiencia de usuario óptima.

9. Cumplimiento con el RGPD:

Appsedu se adhiere estrictamente a las regulaciones del Reglamento General de Protección de Datos (RGPD), garantizando el tratamiento legal, justo y transparente de los datos personales de los usuarios. La plataforma implementa medidas de seguridad robustas y procedimientos claros para proteger la privacidad y los derechos de los usuarios.

Con estas funcionalidades, Appsedu se posiciona como un pilar fundamental en el entorno educativo digital, promoviendo la seguridad, la transparencia y la eficiencia en el uso de las aplicaciones educativas

3.6. Protección de datos en el inicio de sesión

Abordamos la importancia de la protección de datos en las aplicaciones que utilizan mecanismos de inicio de sesión único (SSO) a través de identidades digitales. Estos sistemas requieren un análisis detallado para garantizar el cumplimiento de las normativas de privacidad, en particular el Reglamento General de Protección de Datos (RGPD).

1. ¿Cómo se evalúa la protección de datos en las aplicaciones que utilizan SSO?
   - Se realiza una revisión exhaustiva de la política de privacidad declarada por el editor de la aplicación.
   - Se investiga la ubicación de los servidores para determinar si hay transferencias internacionales de datos.

2. ¿Qué se verifica en relación con las transferencias internacionales de datos?
   - Se analiza si existen decisiones de adecuación de la Comisión Europea para los países receptores.
   - Si no hay decisiones de adecuación, se estudia si la aplicación proporciona garantías adicionales equivalentes a las del RGPD.

3. ¿Qué se considera al evaluar la reputación de una aplicación?
   - Se revisan las cláusulas de la política de privacidad y se verifica la ausencia de problemas previos relacionados con la protección de datos.

4. ¿Cómo se obtiene el consentimiento de los usuarios para transferir sus datos a estas aplicaciones?
   - Se ofrece un formulario donde los usuarios pueden otorgar su consentimiento de manera libre, informada e inequívoca.
   - Las cláusulas de protección de datos se presentan de manera clara y accesible antes de que los usuarios otorguen su consentimiento.

5. ¿Cómo se registra el consentimiento de los usuarios?
   - Cada consentimiento genera un registro en una base de datos, asociando al usuario, la aplicación y la fecha de la operación, entre otros.

6. ¿Cómo pueden los usuarios revocar su consentimiento?
   - Se proporciona un formulario para que los usuarios puedan revocar su consentimiento en cualquier momento.

- La revocación se registra automáticamente en la base de datos.

7. ¿Qué información se almacena en la base de datos de consentimientos?
   - Se almacenan datos como el identificador único del usuario, la aplicación para la que se otorgó el consentimiento, la fecha de la operación y el tipo de transferencia autorizada.
8. ¿Cómo se manejan los consentimientos para diferentes tipos de transferencias?
   - Se distinguen entre las transferencias dentro del Espacio Económico Europeo (EEE), fuera del EEE con garantías equivalentes y fuera del EEE sin garantías equivalentes.

Estas medidas aseguran que las aplicaciones que utilizan SSO cumplan con los requisitos del RGPD, salvaguardando la privacidad y garantizando los derechos de los usuarios en todo momento.

3.7. Datos estadísticos

Tabla 1. Detalle de las aplicaciones analizadas en Appsedu:

	TOTAL	AUTORIZADAS	NO AUTORIZADAS	EN EVALUACIÓN
Aplicaciones en Appsedu	232	194	27	8
Aplicaciones Linux	144	137	5	2
Aplicaciones Windows / MacOS	51	37	12	2
Aplicaciones Android / iOS	29	17	10	2
Aplicaciones WEB (SSO)	5	3	0	2

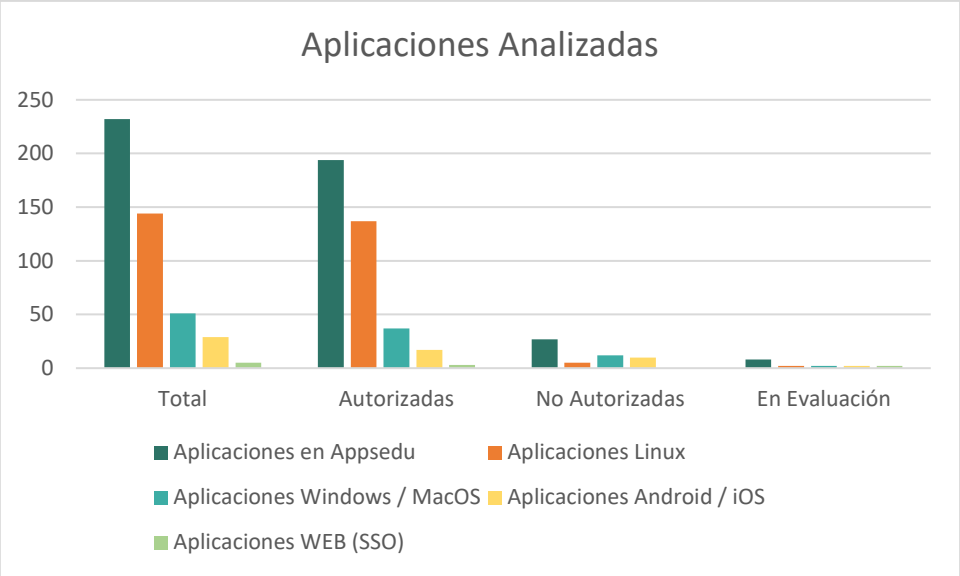


Tabla 2. Detalle de las solicitudes recibidas para análisis en Appsedu:

	SOLICITUDES
Aplicaciones Linux	13
Aplicaciones Windows	115
Aplicaciones MacOS	1
Aplicaciones Android	229
Aplicaciones iOS	4
Aplicaciones SSO	514
Otros tipos	18

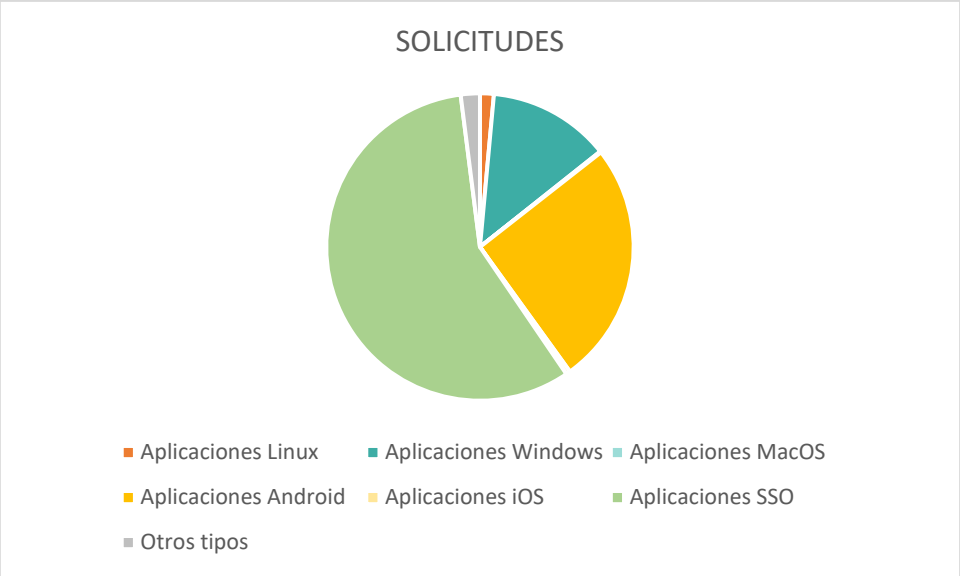


Tabla 3. Identidades Digitales facilitadas por GVA al entorno educativo

USUARIOS	Docentes	No docentes	Alumnado	Centros	TOTAL
ID	79.300	5.979	538.634	1.629	**625.542**

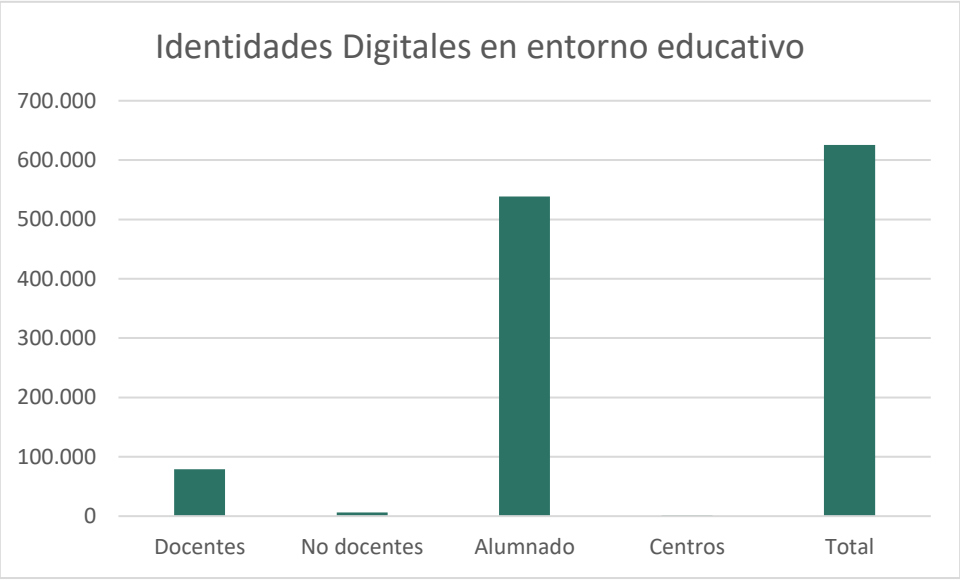


Tabla 4. Las 25 aplicaciones más solicitadas en Appsedu con identificación a través de SSO:

APLICACIONES SSO - TOP 25	SOLICITUDES	APLICACIONES SSO - TOP 25	SOLICITUDES
Canva	5951	TypingClub	385
Apple Internet Accounts	1881	Edpuzzle	325
Kahoot!	1598	Adobe Acrobat Reader	278
Genially	1474	Atlassian	264
SheerID Verification	1207	Additio	248
Blinklearning	962	innovamat-login	242
Padlet	927	Prezi	191
Trimble Identity	680	iDoceo	172
MyFiles	599	AVSantillana O365 Multi-tenant Integration PRO	171
Code.org - Production	570	Lucid	155
Flip	495	Storyboard That	152
Oxford Premium	427	Pixton	147
diagrams.net	392		

4. Repercusión para el ciudadano y las Administraciones

El proyecto de Appsedu tiene una repercusión significativa tanto para los ciudadanos como para las administraciones educativas.

Para los ciudadanos:

- Proporciona un entorno digital seguro al ofrecer un catálogo de aplicaciones educativas evaluadas que cumplen con los estándares de ciberseguridad y protección de datos.
- Permite dar su consentimiento informado para el uso de estas aplicaciones, asegurándoles el control sobre sus datos personales.

Para las Administraciones educativas

- Garantiza el cumplimiento de las normativas de privacidad y ciberseguridad en el uso de aplicaciones en el ámbito educativo.
- Simplifica la gestión de consentimientos y revocaciones, proporcionando un marco claro y estructurado para el manejo de datos sensibles.
- Promueve un uso responsable y seguro de la tecnología en el ámbito educativo.
- Protege la privacidad de los usuarios.
- Ofrece un acceso controlado a aplicaciones que cumplen con los estándares de calidad y seguridad.

5. Equipo de desarrollo y proveedores

El proyecto ha sido impulsado desde la Dirección General de Infraestructuras Educativas dentro de la Conselleria de Educación, Cultura, Universidades y Empleo.

Ha sido dirigido por la Subdirección General de Informática para Educación e Innovación y gestionado y ejecutado por el Servicio de Informática para Centros Educativos.

Han colaborado en el proyecto la Delegación de Protección de Datos de la Comunidad Valenciana y la Subdirección General de Ciberseguridad de la Dirección General de Tecnologías de la Información y las Comunicaciones.

6. Valoración económica

El coste del proyecto por parte de la Dirección General de Infraestructuras Educativas ha sido 97347.50 € (IVA incluido)

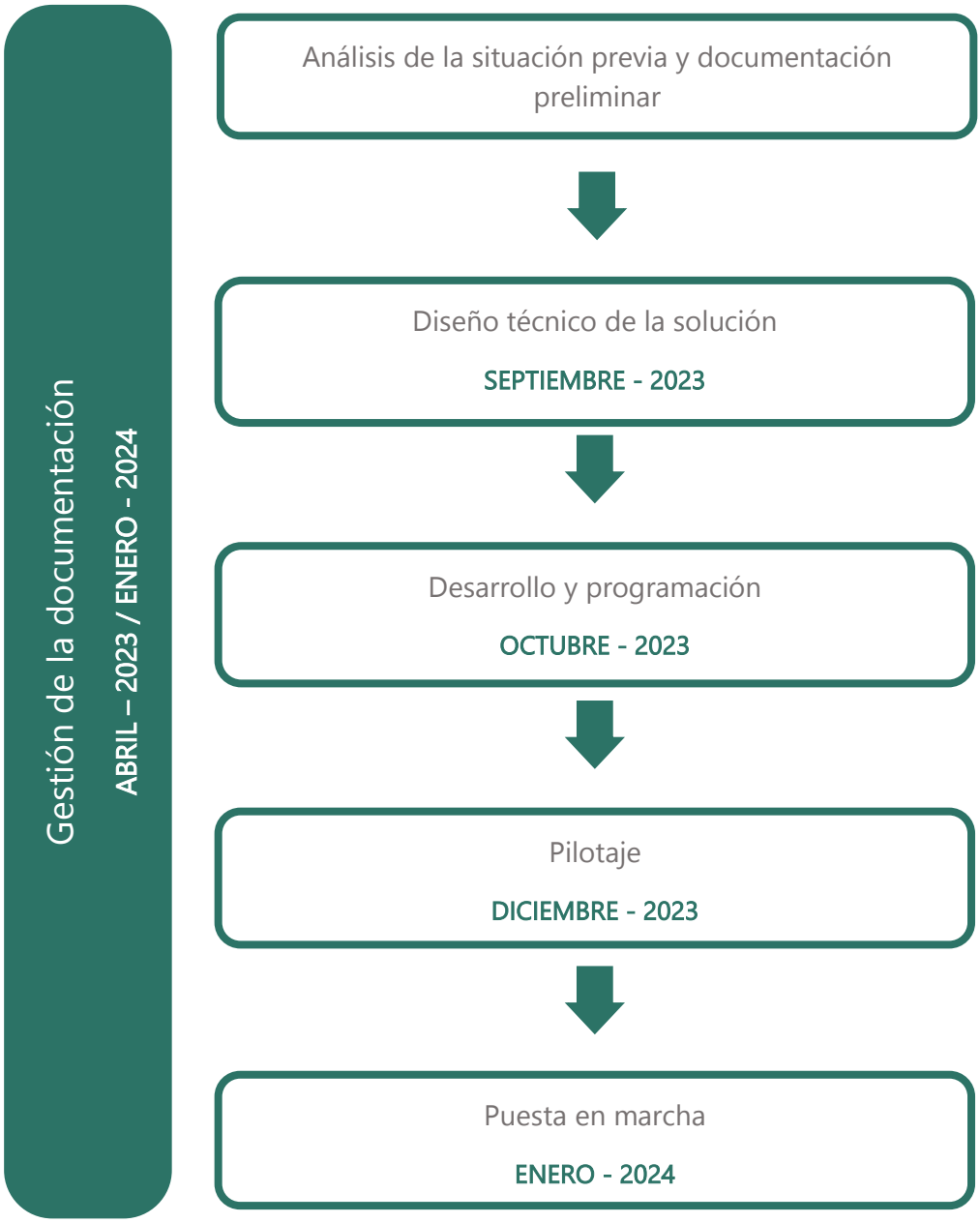
El proyecto incluye las siguientes acciones:

- Auditoría del uso de las aplicaciones en el entorno educativo.
- Estudio e investigación de alternativas.
- Elaboración de los documentos de análisis y diseño.
- Desarrollo de las cláusulas y recomendaciones en protección de datos.

- Implementación de los modelos de datos y herramientas de frontend y backend.
- Análisis de riesgos de seguridad y privacidad de las aplicaciones del catálogo.
- Incorporación de las aplicaciones al catálogo.
- Despliegue en preproducción y acceso limitado al entorno.
- Lanzamiento en producción de la plataforma.

7. Plazos de cumplimiento

A continuación, se desgranan las diferentes fases del proyecto:



La **primera versión operativa** de Appsedu se lanzó el **30 de enero de 2024**, marcando un hito significativo en el esfuerzo continuo de la Conselleria de Educación, Cultura, Universidades y Empleo por mejorar la calidad y seguridad de la educación en la región.

Para el futuro, se prevé el lanzamiento de una nueva versión de Appsedu con funcionalidades adicionales durante el curso escolar 2024-2025, lo que garantizará que la plataforma continúe siendo relevante y eficaz en un entorno educativo en constante evolución.

Appsedu representa el compromiso firme de la Generalitat Valenciana con la excelencia en la educación digital, ofreciendo a la comunidad educativa un entorno seguro y confiable para el aprendizaje y el desarrollo académico.