

**Informe sobre utilización por parte de profesorado
y alumnado de aplicaciones que almacenan datos en nube con
sistemas ajenos a la plataforma educativa institucional del
Gobierno del Principado de Asturias**

Servicio de Inspección Educativa

Marzo 2022



**GOBIERNO DEL
PRINCIPADO DE ASTURIAS**

CONSEJERÍA DE EDUCACIÓN

Tabla de contenido

1	Introducción.....	3
1.1	Normativa	3
1.2	Educativa.....	3
2	Estudio de la AEPD	4
3	Sugerencias y orientaciones.....	5
4	Aplicaciones externas VS institucionales	6
5	Sobre la ubicación de los datos	7
6	Apps que almacenan datos en nube.....	8
6.1	Apps móviles	8
6.2	Entornos de aprendizaje	9
6.3	Herramientas de almacenamiento en nube	9
6.4	Redes sociales	9
6.5	Correo electrónico	10
6.6	Mensajería instantánea	11
7	Plantilla Evaluación de aplicación que almacena datos en nube	12
7.1	Datos de la aplicación	12
7.2	Información básica sobre el tratamiento de datos.....	12
7.3	Permisos de la aplicación	12
7.4	Sobre la ubicación de los datos.....	13
7.5	Observaciones	13
7.6	Prueba de la aplicación	13
7.7	Sobre la seguridad de los datos	14
8	Evaluación de aplicación que almacena datos en nube: Additio	15
8.1	Datos de la aplicación	15
8.2	Información básica sobre el tratamiento de datos.....	15
8.3	Permisos de la aplicación	16
8.4	Sobre la ubicación de los datos.....	17
8.5	Observaciones	17
8.6	Prueba de la aplicación	18
8.7	Sobre la seguridad de los datos	18
9	Evaluación de aplicación que almacena datos en nube: Snappet.....	19
9.1	Datos de la aplicación	19
9.2	Información básica sobre el tratamiento de datos.....	20
9.3	Permisos de la aplicación	20
9.4	Sobre la ubicación de los datos.....	21
9.5	Observaciones	22
9.6	Prueba de la aplicación	22
9.7	Sobre la seguridad de los datos	23
10	Historial de versiones	24

1 Introducción

1.1 Normativa

El **Reglamento General de Protección de Datos** (RGPD) es la normativa que regula la protección de datos de los ciudadanos que vivan en la Unión Europea. El reglamento entró en vigor el 24 de mayo de 2016 y pasó a ser de obligado cumplimiento desde el 25 de mayo de 2018. Conserva parte de la regulación existente -conceptos, principios y derechos de los interesados- pero modifica algunos otros y contiene nuevas obligaciones que habrán de ser cumplidas por los sujetos obligados según sus circunstancias, en este caso, los centros educativos. El nuevo reglamento recoge nuevos derechos a los ciudadanos, información clara, olvido y derecho a la portabilidad.

Por su parte, la **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales**, pretende lograr la adaptación del ordenamiento jurídico español al citado Reglamento y completar sus disposiciones. Establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en ese Reglamento y en esta ley orgánica. Además, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Por último, la **Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia**, recoge en el capítulo XII el papel de la Agencia Española de Protección de Datos, en adelante AEPD, en la protección de datos personales, garantizando los derechos digitales de las personas menores de edad y la retirada inmediata de los contenidos ilícitos.

1.2 Educativa

Los equipos directivos, profesorado, personal administrativo y auxiliar de los centros educativos en el ejercicio de sus funciones y tareas necesitan tratar datos de carácter personal del alumnado y de sus familiares, lo que deberán realizar con la debida diligencia y respeto a su privacidad e intimidad, teniendo presente el interés y la protección de los menores.

Las Administraciones y los centros educativos son los responsables del tratamiento de los datos y deben formar sobre sus principios básicos y cómo hacerlo correctamente.

Con objeto de adecuar el tratamiento de datos de carácter personal a la ley, desde los centros educativos deberán realizarse una serie de actuaciones:

- Revisión de los protocolos internos de autorización de las familias para el uso de los datos personales, autorización de uso de imágenes, etc.
- Revisión de las páginas web y otros servicios en línea, en especial de los protocolos de publicación de información de datos de carácter personal y de recogida de estos en esos medios.
- Revisión de los protocolos de comunicación entre los miembros de la comunidad educativa.

- En especial se revisarán todas aquellas apps que registren datos personales, con almacenamiento en la nube, correo electrónico o redes sociales ajenas a la plataforma institucional -Educastur y Microsoft 365 de Educastur- utilizadas en el entorno escolar por parte de profesorado y alumnado.

En todo caso, para la revisión de los protocolos y servicios utilizados en el centro educativo, deberán seguirse las sugerencias y orientaciones que aporta la AEPD.

Este informe sobre utilización por parte de profesorado y alumnado de aplicaciones que almacenan datos en nube con sistemas ajenos a la plataforma educativa institucional del Gobierno del Principado de Asturias, las recomendaciones que se derivan del mismo y los ejemplos que se incluyen de análisis de dos aplicaciones que guardan datos en nube, se fundamenta en el informe publicado por la AEPD, cuya consulta es complementaria y recomendable:

Informe sobre la utilización por parte de profesorado y alumnado de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas. Orientaciones para centros educativos.

<https://www.aepd.es/media/guias/guia-orientaciones-apps-datos-alumnos.pdf>

También como lecturas complementarias se incluyen las referencias a la Guía sectorial para el ámbito educativo de la propia AEPD y al texto del Reglamento general de protección de datos.

Guía para centros educativos. Guías sectoriales AEPD.

<http://www.tudecideseninternet.es/agpd1/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf>

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

<https://www.boe.es/doue/2016/119/L00001-00088.pdf>

2 Estudio de la AEPD

El estudio de la AEPD tiene su origen y justificación en el fuerte incremento del uso de apps en el entorno escolar por parte de profesorado y alumnado, así como el gran volumen de datos personales que se manejan.

- El informe destaca que se utilizan apps, almacenamiento en nube, correo electrónico o redes sociales ajenas a las plataformas de los centros (institucionales) y que, en muchos casos, podría existir un riesgo de pérdida de control sobre los datos personales que se aportan.
- El documento incluye orientaciones y un decálogo de recomendaciones para fomentar la protección de datos a través del buen uso de las aplicaciones en los centros docentes.

El cuestionario online en el que se basó el informe recababa información sobre los siguientes aspectos relativos al uso de las apps tanto por el alumnado a instancias del profesorado, como por el propio profesorado:

- Aplicaciones para el aula en dispositivos tales como móviles, tabletas o portátiles.
- Herramientas de almacenamiento en nube (tipo Dropbox, Google Drive, etc.).
- Redes sociales (Facebook, Instagram, etc.), para trabajos colaborativos u otro tipo de trabajos en el aula.
- Correo electrónico para el intercambio de información entre alumnado, familias y profesorado.
- Existencia en los centros de normas internas y procedimientos con relación al uso de estas aplicaciones.

3 Sugerencias y orientaciones

Del citado estudio, la AEPD ha elaborado un decálogo de sugerencias y orientaciones.

- Los centros educativos deben velar por que la incorporación de las tecnologías en las aulas se realice respetando el derecho a la protección de datos de aquellos cuya información personal se trata.
- Los centros deben utilizar únicamente aquellas aplicaciones que ofrezcan información claramente definida sobre quién trata los datos, para qué y con qué finalidad, así como dónde se almacenan, el tiempo que se guardan y las medidas de seguridad.
- La política de seguridad de los centros debe incluir las aplicaciones utilizadas y el profesorado debe solicitar autorización para su uso al centro, el cual debe hacer una evaluación de la aplicación en materia de seguridad de la información. Deben establecerse procedimientos que obliguen a solicitar la autorización del centro para el uso de estas aplicaciones.
- Los centros deben informar de manera sencilla y transparente a las familias o tutores sobre la utilización de la tecnología en las aulas, así como de las apps que utilicen para tratar datos personales del alumnado.
- Las aplicaciones utilizadas deben permitir el control por parte de los tutores y las tutoras o profesorado de los contenidos subidos por los y las menores, y en especial de los contenidos multimedia.
- Debe tenerse especial cuidado con la publicación de fotografías o vídeos de alumnado facilitados por terceros, tales como otro alumnado o profesorado.
- Deben establecerse programas informativos de concienciación para profesorado y alumnado sobre protección de datos y la importancia del uso correcto de aplicaciones, sobre todo en lo concerniente a la publicación de imágenes y vídeos, configuración de opciones de privacidad o uso de contraseñas robustas, entre otros.
- Al utilizar sistemas de almacenamiento en nube se debe evitar incluir especialmente datos de salud, contraseñas, datos bancarios o material audiovisual de contenido sensible.
- Cuando exista en el centro una plataforma educativa que permita la interacción entre el alumnado, y entre este y el profesorado, se aconseja que se prime su utilización para este fin, sin establecer mecanismos de comunicación adicionales.
- Para los casos de tratamientos especiales de datos que puedan suponer un mayor riesgo, tal como el reconocimiento facial de menores de edad, el centro docente debe

obtener el consentimiento expreso del alumnado (si son mayores de 14 años) o de las familias o tutores (si son menores de 14 años) y asegurarse de la finalidad para la que se utilizan.

En ningún caso se prohíbe directamente el uso de este tipo de aplicaciones. Cada una de ellas debe ser analizada bajo las premisas indicadas y actuar en consecuencia.

Parte de las acciones que se deben tomar están dentro de la autonomía de los centros. Es previsible que la situación que se plantea tras la publicación de este informe, y ante el proceso de adaptación a la ley, provoque desconcierto en los centros educativos.

Con todo ello, desde el Servicio de Inspección Educativa se ha considerado conveniente estudiar algunas de las herramientas más populares en nuestros centros entre profesorado y alumnado, analizando su uso, posibles alternativas institucionales y acciones recomendadas en el nuevo contexto que se plantea dentro del ámbito de la protección de datos. Se incluyen como anexos un modelo de plantilla para análisis de aplicaciones que guardan datos en nube y dos ejemplos de análisis de aplicación de este tipo siguiendo ese modelo. Estos dos ejemplos se proporcionan exclusivamente con este fin y no son recomendaciones en ningún caso. Cada centro debe decidir sobre su uso en función de sus requisitos y hacer su propia valoración en el momento de tomar la decisión.

4 Aplicaciones externas VS institucionales

En este informe se consideran aplicaciones *externas* o *de terceros* todas aquellas que no son proporcionadas directamente a los centros educativos por la Consejería de Educación y por la Consejería competente en materia de gestión de los sistemas de información corporativos del Gobierno del Principado de Asturias. Las proporcionadas directamente se conocen en este informe como *institucionales* o *corporativas*.

Las aplicaciones externas están realizadas por terceros ajenos a la Consejería de Educación. La Consejería no pone a disposición, ni siquiera recomienda, el uso de aplicaciones de terceros. Pero tal como se recoge en el apartado anterior, en ningún caso se prohíbe directamente su uso. Cada una de ellas debe ser analizada bajo las premisas indicadas y actuar en consecuencia. El centro y el profesorado que las utilizan son responsables de los datos suministrados a estas aplicaciones, y deberán seguir escrupulosamente la normativa vigente sobre protección de datos.

Los centros y el profesorado emplearán preferiblemente los servicios educativos en línea que proporciona la Consejería de Educación, desde el correo institucional y las aplicaciones en la nube de Microsoft 365, hasta las Aulas virtuales o el portal de webs de centros (alojaweb), entre otros, que constituyen un marco institucional y seguro.

La utilización de determinados servicios de Educastur implicará asimismo la aceptación, sin reserva alguna, de sus condiciones de uso y servicio generales y particulares, cuya lectura es recomendable:

- <https://www.educastur.es/condiciones-de-uso>
- <https://sway.office.com/N9fAoJClqouqBsFb>

5 Sobre la ubicación de los datos

Los datos deben estar almacenados en un país del Espacio Económico Europeo o un país que ofrezca un nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea). Puede consultarse la lista de países con nivel adecuado de protección en los siguientes enlaces:

- [Sede Electrónica - Agencia Española de Protección de Datos - Preguntas Frecuentes \(sedeagpd.gob.es\)](https://sedeagpd.gob.es)
- [Adequacy decisions | European Commission \(europa.eu\)](https://eudataprivacy.europa.eu/)

La sentencia del Tribunal de Justicia de la Unión Europea (TJUE) invalidó la [Decisión \(UE\) 2016/1250 de la Comisión, de 12 de julio de 2016](#) conocida como *Escudo de Privacidad*, o *Privacy Shield*, al que se acogía la versión anterior de este informe para reconocer los países con nivel de protección equivalente al europeo.

“El Tribunal ha invalidado la Decisión Escudo de la privacidad sin mantener sus efectos, ya que la legislación estadounidense evaluada por el Tribunal no proporciona un nivel de protección sustancialmente equivalente al garantizado en la UE. Esta evaluación debe tenerse en cuenta para cualquier transferencia a los EE.UU.

Las transferencias basadas en este marco jurídico son ilegales. Si desea seguir transfiriendo datos a los Estados Unidos, deberá comprobar si puede hacerlo en las condiciones que se exponen.”

Las empresas que suministren los servicios que se oferten a los centros educativos deben asegurar ese nivel de seguridad y protección requerido, asumiendo las Cláusulas Contractuales Tipo (“SCCs”) aprobadas por la Comisión Europea el 4 de junio del 2021. Estas nuevas SCCs sustituyen a las cláusulas previamente aprobadas en la Directiva 95/46/EC.

Microsoft y Google aplican las cláusulas contractuales estándar como base para la transferencia de datos para sus servicios en línea para educación, además de ubicar sus servicios y datos en centros de datos situados en la Unión Europea.

La Consejería de Educación del Gobierno del Principado de Asturias hospeda localmente la plataforma *Moodle* a través de sus servicios *Campus* (*Campus Aulas virtuales*, *Campus Formación* y *Campus FP distancia*).

6 Apps que almacenan datos en nube

6.1 Apps móviles¹

Aplicación	Tipo	Alternativa corporativa	Acción recomendada
Additio	Organizador docente	No existe	Evaluar
iDoceo	Organizador docente	No existe	Evaluar
Evernote	Bloc de notas	OneNote Microsoft 365 Educación	Sustituir
Apple Notas	Bloc de notas	OneNote Microsoft 365 Educación	Sustituir
Google Keep	Bloc de notas	OneNote Microsoft 365 Educación	Sustituir
SlideShare	Presentaciones	Sway y PowerPoint Microsoft 365 Educación	Sustituir
Kahoot	Gamificación	No existe como tal. Parcialmente cubierta con Forms Microsoft 365 Educación	Evaluar
Mindomo	Mapas conceptuales	Visio y Whiteboard Microsoft 365 Educación	Sustituir
Pixton	Cómics	No existe	Evaluar
Flipgrid²	Video conversación	Parcialmente cubierta con Stream Microsoft 365 Educación	Evaluar

En este apartado se incluyen no solo las apps para dispositivos móviles sino también las aplicaciones web. Debido su elevado número y a que todas ellas son herramientas con finalidad muy específica, no suelen existir alternativas corporativas que las puedan sustituir. Por ello deberán evaluarse y someterse al proceso de autorización y, en la medida de lo posible, utilizar cuentas genéricas (sin incluir datos reales de alumnado) para su uso.

Acciones recomendadas

- Evaluar siguiendo el guion sugerido en el informe.
- Autorizar a nivel de centro si la aplicación supera la evaluación.
- Incluir en la política de seguridad.
- Informar al claustro, indicando que, independientemente de la superación de la evaluación, se debe evitar incluir datos personales sensibles.

¹ Este listado no pretende ser exhaustivo. Existe un número muy elevado de aplicaciones que hace imposible recogerlas todas. Las citadas aparecen como ejemplo.

² *Flipgrid* ha sido adquirida por Microsoft, pero en el momento de redactar este informe no está integrado en Microsoft 365 Educación. Es una app/servicio muy popular en la enseñanza de idiomas, pero su cobertura legal y adaptación a la norma europea de protección de datos en el momento de redacción de este informe no es óptima.

- Informar a las familias de su uso.

Las aplicaciones que más datos personales del alumnado pueden llegar a tratar son los cuadernos de notas del personal docente, que mantienen el progreso, calificaciones y observaciones del alumnado. Dadas las funcionalidades que ofrecen estas aplicaciones y la tipología de los datos que tratan, los tratamientos efectuados podrían incluir la elaboración de perfiles de aprendizaje, preferencias o comportamiento de menores de edad por parte de los responsables de las aplicaciones.

6.2 Entornos de aprendizaje

Aplicación	Tipo	Alternativa corporativa	Acción recomendada
Moodle	LMS	Educastur Aulas Virtuales Teams Microsoft 365 Educación	Sustituir
Edmodo	LMS	Educastur Aulas Virtuales Teams Microsoft 365 Educación	Sustituir
Google Classroom	LMS	Educastur Aulas Virtuales Teams Microsoft 365 Educación	Sustituir

6.3 Herramientas de almacenamiento en nube

Aplicación	Tipo	Alternativa corporativa	Acción recomendada
Dropbox	Almacenamiento archivos	OneDrive Microsoft 365 Educación	Sustituir
Google Drive	Almacenamiento archivos	OneDrive Microsoft 365 Educación	Sustituir
iCloud	Almacenamiento archivos	OneDrive Microsoft 365 Educación	Sustituir
Google Fotos	Almacenamiento fotografías	OneDrive/Sway Microsoft 365 Educación	Sustituir
iCloud Fotos	Almacenamiento fotografías	OneDrive/Sway Microsoft 365 Educación	Sustituir
Flickr	Almacenamiento fotografías	OneDrive/Sway Microsoft 365 Educación	Sustituir
Instagram	Almacenamiento fotografías	OneDrive/Sway Microsoft 365 Educación	Sustituir
YouTube	Almacenamiento vídeos	Stream Microsoft 365 Educación	Sustituir

Son utilizadas tanto por el profesorado como por el alumnado con la finalidad fundamental de compartir documentos, normalmente apuntes de clase y materiales didácticos en general, así como trabajos del alumnado. Pero también se da la utilización de estas herramientas para almacenar datos personales tales como listas de asistencia, calificaciones, fotos y vídeos.

6.4 Redes sociales

Aplicación	Tipo	Alternativa corporativa	Acción recomendada
Facebook	Red social	No existe como entorno abierto	Evaluar

Twitter	Red social	No existe como entorno abierto	Evaluar
Instagram	Red social	No existe como entorno abierto. También ofrece almacenamiento de fotografías (ver más arriba)	Evaluar

El uso de las redes sociales suele satisfacer dos necesidades en los centros educativos.

1. Divulgación de las actividades de los centros. La gran entrada de estas redes sociales entre los usuarios finales, especialmente Facebook, contando entre ellos a las familias del alumnado, las hace una excelente plataforma para ese fin. La comunicación y difusión, en algunos casos, es bidireccional, al permitir interactuar con las familias.
2. Uso didáctico, en forma de proyectos educativos donde el factor motivador de la herramienta tiene un gran peso.

6.5 Correo electrónico

Aplicación	Tipo	Alternativa corporativa	Acción recomendada
gmail.com	Correo electrónico	Outlook Microsoft 365 Educación	Sustituir
outlook.es outlook.com hotmail.com	Correo electrónico	Outlook Microsoft 365 Educación	Sustituir
icloud.com me.com	Correo electrónico	Outlook Microsoft 365 Educación	Sustituir
yahoo.com yahoo.es	Correo electrónico	Outlook Microsoft 365 Educación	Sustituir

El uso del servicio de correo electrónico en los centros está generalizado, especialmente entre el profesorado. En los dos últimos cursos escolares, el correo institucional de Educastur ha avanzado significativamente en su implantación para cualquier comunicación con la comunidad docente, abandonándose progresivamente el uso de servicios públicos y comerciales como los reseñados en la tabla. Debe continuar separándose el correo electrónico personal del corporativo, si bien es posible utilizar el corporativo para cuestiones particulares respetando las condiciones establecidas en sus condiciones de uso, disponibles en la dirección <https://sway.office.com/N9fAoJClqouqBsFb>:

“El uso privado de la cuenta de correo se limitará a cuestiones personales o domésticas, siempre que no sea abusivo y que no perjudique la seguridad del servicio ni el normal desarrollo de la acción docente, discente o profesional.”

No está permitido el uso del correo corporativo para actividades profesionales o contratación de servicios ajenos a la actividad educativa o profesional o cualquier actividad que implique beneficio personal o ánimo de lucro.”

Más allá de redirecciones, se recomienda el uso de la configuración directa de la cuenta en el cliente preferido por el usuario o, aún mejor, la instalación de un segundo cliente de correo electrónico, preferiblemente *Microsoft Outlook*, para atender el correo corporativo.

En ocasiones se utiliza el correo electrónico para mandar informes tutoriales entre el profesorado. En este caso ambos docentes deberían estar usando la plataforma corporativa.

Cuentas válidas

- educastur.org (profesorado)
- educastur.es (alumnado)

6.6 Mensajería instantánea

Aplicación	Tipo	Alternativa corporativa	Acción recomendada
WhatsApp	Mensajería	Teams Microsoft 365 Educación	Sustituir
Telegram	Mensajería	Teams Microsoft 365 Educación	Sustituir
Hangouts	Mensajería	Teams Microsoft 365 Educación	Sustituir
Skype	Mensajería	Teams Microsoft 365 Educación	Sustituir ³
TokApp School	Notificación escolar	No existe	Evaluar
EdVoice	Notificación escolar	No existe	Evaluar

El tipo de uso de este tipo de aplicaciones es variado. Suele cubrir la comunicación entre profesorado, entre profesorado y alumnado y, en algunos casos, entre profesorado y familias. El uso entre familias no se analiza aquí.

Las mejoras que se han venido introduciendo en *Microsoft Teams* permiten que actualmente no tenga limitaciones para un uso educativo amplio. Por ejemplo, para encuentros con profesorado/alumnado de fuera de la comunidad/país, necesidad que se da frecuentemente en proyectos europeos, asociaciones escolares, etc. Es de destacar aquí el esfuerzo de Microsoft por ofrecer el acceso a Invitados, usuarios externos a la organización con cualquier tipo de cuenta o de forma anónima compartiendo el enlace a la reunión.

Mención especial merecen *TokApp School* <https://www.tokappschool.com> y *Additio EdVoice* <http://www.additioapp.com/es/edvoice> como soluciones globales de comunicación con las familias. Estas aplicaciones llegan incluso a integrar los organizadores docentes comentados en el primer apartado. En este mismo tipo de aplicaciones se encuentran *Smart Schools* <https://www.smartschools.network>, *Alexia* <http://www.alexiaeducacion.com>, *Click Edu* <https://clickartedu.com> y otras. Todas ellas requerirían una evaluación exhaustiva para determinar el alcance de datos implicados en la interacción con las familias y la forma de disponer el contacto con estas, debiendo considerarse en este último caso la provisión de los datos y el necesario consentimiento para ella.

³ El servicio de *Skype* está siendo sustituido por *Teams*, tanto en su vertiente corporativa como personal.

7 Plantilla Evaluación de aplicación que almacena datos en nube

Centro educativo	
Fecha de la evaluación	
Resultado de la evaluación	
Apartados no superados	

7.1 Datos de la aplicación

Sitio web	
Política de privacidad	
Nota Legal	

7.2 Información básica sobre el tratamiento de datos

Se debe comprobar si el responsable de la aplicación informa claramente de:

Apartado	Informa	Información
Identidad del responsable	Sí / No	
Dirección del responsable	Sí / No	
Finalidades de los datos	Sí / No	
Comunicaciones de datos a terceros	Sí / No	
Identidad de terceros	Sí / No	
Finalidad de la cesión a terceros	Sí / No	
Derechos que asisten a los titulares de los datos	Sí / No	
Periodos de conservación de los datos	Sí / No	
Medidas de seguridad facilitadas	Sí / No	

Nota: Esta información debería estar fácilmente accesible en la política de seguridad y nota legal de la aplicación. En caso de que falte alguno de estos aspectos, o que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.

7.3 Permisos de la aplicación

Informa de posibles accesos a los datos del dispositivo o a sus sensores	Sí / No
---	---------

Detalle de los accesos

Apartado	Información
Identidad	
Calendario	
Contactos	
Teléfono	
Fotos/multimedia/archivos	
Almacenamiento	

Micrófono	
Información sobre la conexión Wi-Fi	
ID de dispositivo y datos de llamada	
Otros	

Nota: Esta información debería estar accesible en las correspondientes tiendas de aplicaciones o en su web. En caso de que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.

7.4 Sobre la ubicación de los datos

País y/o empresa	EU	EQ	EU-US

EU: País del Espacio Económico Europeo

EQ: País con nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea). Puede consultar la lista de países con nivel adecuado de protección en los siguientes enlaces.

- [Sede Electrónica - Agencia Española de Protección de Datos - Preguntas Frecuentes \(sedeagpd.gob.es\)](https://sedeagpd.gob.es)
- [Adequacy decisions / European Commission \(europa.eu\)](https://eudataprivacy.europa.eu/)

EU-US: Los datos también pueden localizarse en empresas ubicadas en Estados Unidos siempre que estas hayan formalizado los contratos modelo prescritos por la Comisión Europea (cláusulas contractuales estándar) que garanticen un nivel de protección equivalente.

En cualquier otro caso, se recomienda solicitar información sobre las posibles transferencias internacionales de datos y las garantías de su licitud, en particular sobre las que necesitan autorización por parte de la Agencia Española de Protección de Datos.

7.5 Observaciones

7.6 Prueba de la aplicación

Se considera conveniente poner a prueba la aplicación de forma previa a su definitiva utilización en el centro, realizando la prueba sin introducir datos personales reales de los alumnos ni involucrarlos en su utilización. En esta fase de prueba se debería comprobar la corrección de las informaciones que fueron facilitadas por el responsable de la aplicación.

7.7 Sobre la seguridad de los datos

La responsabilidad del cumplimiento de las medidas de seguridad debe entenderse siempre compartida entre los diferentes actores intervinientes (responsable de la aplicación, centro educativo y usuarios), debiendo en todo caso el responsable de la aplicación facilitar las medidas técnicas adecuadas para garantizar la seguridad de los datos tratados, y el centro aplicarlas o utilizarlas correctamente, además de implementar las medidas organizativas apropiadas.

Así, por ejemplo, la aplicación debe proveer mecanismos que permitan la realización de copias de seguridad o la descarga de los datos, de tal forma que el centro pueda cumplir con las obligaciones que le son exigibles al respecto, introduciendo en su política de seguridad la realización de copias de seguridad de los datos tratados mediante estas aplicaciones, y realizando efectivamente la realización de dichas copias.

La responsabilidad de las medidas de identificación de usuarios también es compartida. Por un lado, la aplicación debe implementar un mecanismo de autenticación que permita la identificación inequívoca y personalizada de los usuarios, recomendándose que este mecanismo consista en códigos de usuario y contraseñas, evitando la identificación de menores mediante datos biométricos (reconocimiento facial o huella dactilar).

Si se utilizan contraseñas, el centro debe incluir en su política el cambio periódico de las mismas, por lo que las aplicaciones que se vayan a utilizar deben incluir mecanismos para permitir dichos cambios. A los usuarios les corresponde la obligación de utilizar contraseñas fuertes y custodiarlas sin desvelarlas a terceros.

8 Evaluación de aplicación que almacena datos en nube: Additio

Nota: Este análisis se proporciona a modo de ejemplo y no supone que la aplicación analizada sea recomendada en ningún caso. Cada centro debe decidir sobre su uso y hacer su propia valoración en el momento de tomar la decisión.

Centro educativo	Consejería de Educación
Fecha de la evaluación	Octubre 2021
Resultado de la evaluación	Favorable
Apartados no superados	

8.1 Datos de la aplicación

Nombre	Additio
Sitio web	http://www.additioapp.com/es/
Política de privacidad	http://www.additioapp.com/es/seguridad-y-privacidad/
Nota Legal	http://www.additioapp.com/es/nota-legal/

8.2 Información básica sobre el tratamiento de datos

Se debe comprobar si el responsable de la aplicación informa claramente de:

Apartado	Informa	Información
Identidad del responsable	Sí	DIDACTIC LABS S.L. NIF: B55240162
Dirección del responsable	Sí	C/ Bescanó, 10. 17007 Girona. España Teléfono: +34 972 39 32 40 Email: info@additioapp.com
Finalidades de los datos	Sí	Ofrecer y gestionar nuestros servicios y productos para el sector educativo.
Comunicaciones de datos a terceros	Sí	A las administraciones públicas, siempre que lo exija la legislación vigente, y a todas aquellas entidades cuando sea necesario.
Identidad de terceros	Sí	Administraciones públicas. Otras entidades cuando sea necesario.
Finalidad de la cesión a terceros	Sí	Cumplir con la legislación vigente. Cumplir con la finalidad del tratamiento.
Derechos que asisten a los titulares de los datos	Sí	Cualquier persona tiene derecho a obtener confirmación sobre si en Additio App están tratando datos personales que les conciernan, o no. Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos. En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo

		caso únicamente los conservarán para el ejercicio o la defensa de reclamaciones. En determinadas circunstancias y por motivos relacionados con su situación particular, los interesados podrán oponerse al tratamiento de sus datos. Additio App dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones. Los interesados tienen derecho a la portabilidad de sus datos. Finalmente, los interesados pueden dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.
Periodos de conservación de los datos	Sí	Mientras los interesados usen Additio App. El no uso de la aplicación durante un largo periodo de tiempo (12 meses) hace que pierda su finalidad y se procede a eliminar la cuenta y los datos asociados a ella.
Medidas de seguridad facilitadas	Sí	Aplica las medidas de seguridad exigidas, de conformidad con el artículo 32 del RGPD, para garantizar un nivel de seguridad adecuado al riesgo del tratamiento de datos que realizan, con mecanismos que permiten garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento.

Additio adopta políticas internas y aplica medidas para cumplir los estándares de privacidad, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (RGPD), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (LOPDGDD).

Nota: Esta información debería estar fácilmente accesible en la política de seguridad y nota legal de la aplicación. En caso de que falte alguno de estos aspectos, o que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.

8.3 Permisos de la aplicación

Informa de posibles accesos a los datos del dispositivo o a sus sensores	Sí
---	----

Detalle de los accesos

Apartado	Información
Identidad	buscar cuentas en el dispositivo añadir o eliminar cuentas
Calendario	leer eventos de calendario e información confidencial añadir o modificar eventos de calendario y enviar mensajes a los invitados sin el consentimiento de los propietarios
Contactos	buscar cuentas en el dispositivo
Teléfono	consultar la identidad y el estado del teléfono

Fotos/multimedia/archivos	leer el contenido de tu almacenamiento USB modificar o eliminar contenido del almacenamiento USB
Almacenamiento	leer el contenido de tu almacenamiento USB modificar o eliminar contenido del almacenamiento USB
Micrófono	grabar sonido
Información sobre la conexión Wi-Fi	ver conexiones Wi-Fi
ID de dispositivo y datos de llamada	consultar la identidad y el estado del teléfono
Otros	recibir datos de Internet ver conexiones de red crear cuentas y establecer contraseñas acceso completo a red usar cuentas del dispositivo

Nota: Esta información debería estar accesible en las correspondientes tiendas de aplicaciones o en su web. En caso de que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.

8.4 Sobre la ubicación de los datos

País y/o empresa	EU	EQ	EU-US
Hetzner Online GmbH (Alemania)	Sí		
Amazon Web Services EMEA, SARL	Sí		
Google Firebase, Google Ireland Limited	Sí		

EU: País del Espacio Económico Europeo

EQ: País con nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea). Puede consultar la lista de países con nivel adecuado de protección en los siguientes enlaces.

- [Sede Electrónica - Agencia Española de Protección de Datos - Preguntas Frecuentes \(sedeagpd.gob.es\)](https://sedeagpd.gob.es/)
- [Adequacy decisions / European Commission \(europa.eu\)](https://eudataprivacy.eu/)

EU-US: Los datos también pueden localizarse en empresas ubicadas en Estados Unidos siempre que estas hayan formalizado los contratos modelo prescritos por la Comisión Europea (cláusulas contractuales estándar) que garanticen un nivel de protección equivalente.

En cualquier otro caso, se recomienda solicitar información sobre las posibles transferencias internacionales de datos y las garantías de su licitud, en particular sobre las que necesitan autorización por parte de la Agencia Española de Protección de Datos.

8.5 Observaciones

Additio se integra con Google, Microsoft y Moodle. Google y Microsoft aplican las cláusulas contractuales estándar como base para la transferencia de datos para sus servicios en línea para educación, además de ubicar sus servicios y datos en centros de datos situados en la Unión

Europea. La Consejería de Educación del Gobierno del Principado de Asturias hospeda localmente la plataforma Moodle a través de sus servicios Campus (Campus Aulas virtuales, Campus Formación y Campus FP distancia).

Additio tiene una funcionalidad aparte llamada *EdVoice*.

En ambos casos habría que evaluar cada una de esas funcionalidades como aplicación independiente ya que *Additio* puede funcionar sin hacer uso de ambas.

8.6 Prueba de la aplicación

Se considera conveniente poner a prueba la aplicación de forma previa a su definitiva utilización en el centro, realizando la prueba sin introducir datos personales reales del alumnado ni involucrarlo en su utilización. En esta fase de prueba se debería comprobar la corrección de las informaciones que fueron facilitadas por el responsable de la aplicación.

8.7 Sobre la seguridad de los datos

La responsabilidad del cumplimiento de las medidas de seguridad debe entenderse siempre compartida entre los diferentes actores intervinientes (responsable de la aplicación, centro educativo y usuarios), debiendo en todo caso el responsable de la aplicación facilitar las medidas técnicas adecuadas para garantizar la seguridad de los datos tratados, y el centro aplicarlas o utilizarlas correctamente, además de implementar las medidas organizativas apropiadas.

Así, por ejemplo, la aplicación debe proveer mecanismos que permitan la realización de copias de seguridad o la descarga de los datos, de tal forma que el centro pueda cumplir con las obligaciones que le son exigibles al respecto, introduciendo en su política de seguridad la realización de copias de seguridad de los datos tratados mediante estas aplicaciones, y realizando efectivamente la realización de dichas copias.

La responsabilidad de las medidas de identificación de usuarios también es compartida. Por un lado, la aplicación debe implementar un mecanismo de autenticación que permita la identificación inequívoca y personalizada de los usuarios, recomendándose que este mecanismo consista en códigos de usuario y contraseñas, evitando la identificación de menores mediante datos biométricos (reconocimiento facial o huella dactilar).

Si se utilizan contraseñas, el centro debe incluir en su política el cambio periódico de las mismas, por lo que las aplicaciones que se vayan a utilizar deben incluir mecanismos para permitir dichos cambios. A los usuarios les corresponde la obligación de utilizar contraseñas fuertes y custodiarlas sin desvelarlas a terceros.

9 Evaluación de aplicación que almacena datos en nube: Snappet

Nota: Este análisis se proporciona a modo de ejemplo y no supone que la aplicación analizada sea recomendada en ningún caso. Cada centro debe decidir sobre su uso y hacer su propia valoración en el momento de tomar la decisión.

Centro educativo	Consejería de Educación
Fecha de la evaluación	Octubre 2021
Resultado de la evaluación	Favorable
Apartados no superados	

9.1 Datos de la aplicación

Nombre	Snappet
Sitio web	https://es.snappet.org
Política de privacidad	https://es.snappet.org/terminos-y-condiciones/
Nota Legal	Incluida en el enlace anterior. Se proporcionan dos direcciones de correo electrónico para completar información: legal@snappet.org y privacy@snappet.org

Enlaces complementarios

Política de privacidad y datos

<https://es.snappet.org/wp-content/uploads/2021/10/Privacy-cookie-statement-website-Snappet-ES-2.1-20201216.pdf>

Términos de uso

<https://es.snappet.org/wp-content/uploads/2021/10/Total-contract-Snappet-ES-20200508.pdf>

Acuerdo de tratamiento de datos

<https://colegios.snappet.org/wp-content/uploads/2018/05/180516-Acuerdo-tratamiento-de-datos-FINAL.pdf>

Snappet empresa

Snappet es un desarrollador de aplicaciones informáticas sobre contenidos educativos, cuyo objetivo principal es el de mejorar la calidad de la educación primaria, de niños menores de catorce años, mediante una solución basada en la enseñanza a través de tabletas. En este contexto, Snappet suscribe acuerdos con centros de enseñanza para suministrarles tabletas y hardware afín que incorpora contenidos educativos desarrollados por Snappet. Adicionalmente, a través de sus instructores, presta asesoramiento al profesorado de los centros educativos sobre el uso y posibilidades de explotación de las herramientas educativas.

Snappet método

Snappet permite recopilar y analizar el número de actividades que realiza el alumno y su progreso en cada área (Matemáticas, Lengua e Inglés). Se hace énfasis en las áreas donde el

alumno tiene más necesidades y se adapta a la forma y al ritmo de aprendizaje de cada uno, creando una ruta de enseñanza personalizada y única para cada estudiante.

Para que este proceso mejore los resultados, *Snappet* propone una estructura lógica de los objetivos y basado en el aprendizaje para el dominio (*Mastery Learning*).

9.2 Información básica sobre el tratamiento de datos

Se debe comprobar si el responsable de la aplicación informa claramente de:

Apartado	Informa	Información
Identidad del responsable	Sí	Snappet España, S.L. NIF B86877800. Empresa europea con presencia en Holanda, Alemania, Francia, Italia y España.
Dirección del responsable	Sí	Piamonte 23. Madrid (28004). Teléfono 0034 91 489 66 94 soporte@snappet.org
Finalidades de los datos	Sí	Snappet solo procesa los datos de personas de contacto de Colegios y profesores y/o personas de contacto que usan los servicios de Snappet.
Comunicaciones de datos a terceros	Sí	Snappet no proporciona, vende ni alquila los datos que procesa a terceros, a menos que Snappet esté legalmente obligado a hacerlo o si se ha otorgado permiso para ello.
Identidad de terceros	Sí	Proveedores de servicios (procesadores).
Finalidad de la cesión a terceros	Sí	Estos procesadores no procesan los datos para sus propios fines, sino solamente en nombre de <i>Snappet</i> .
Derechos que asisten a los titulares de los datos	Sí	Información e inspección, rectificación, olvido, objeción, portabilidad de datos. Información y reclamación de estos.
Periodos de conservación de los datos	Sí	Información de contacto: un máximo de 4 semanas después de procesar una solicitud o solicitud de información. Para los clientes, se aplica un período de retención de no más de 7 años después del final del acuerdo. Datos financieros: hasta 7 años en relación con el período de almacenamiento fiscal.
Medidas de seguridad facilitadas	Sí	Medidas técnicas y organizativas. Regularmente evaluadas, ajustadas y, si es necesario, actualizadas. Sitio web protegido a través de conexión segura.

Nota: Esta información debería estar fácilmente accesible en la política de seguridad y nota legal de la aplicación. En caso de que falte alguno de estos aspectos, o que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.

9.3 Permisos de la aplicación

Informa de posibles accesos a los datos del dispositivo o a sus sensores	NA
--	----

No parece tener una aplicación propia, se trata de una aplicación web. *Snappet* es compatible con cualquier dispositivo que disponga de una conexión a Internet.

El alumnado puede conectarse a la plataforma de *Snappet* desde su teléfono, su iPad, su propia tableta u ordenador y dirigirse a la página <https://alumno.snappet.org>.

El profesorado accede a su cuadro de mando en la dirección <https://profe.snappet.org>.

Detalle de los accesos (*no aplicable*)

Apartado	Información
Identidad	
Calendario	
Contactos	
Teléfono	
Fotos/multimedia/archivos	
Almacenamiento	
Micrófono	
Información sobre la conexión Wi-Fi	
ID de dispositivo y datos de llamada	
Otros	

Nota: Esta información debería estar accesible en las correspondientes tiendas de aplicaciones o en su web. En caso de que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.

9.4 Sobre la ubicación de los datos

Snappet almacena los datos de carácter personal dentro de la UE (EEE). Recurre a terceros para cumplir sus objetivos y requisitos legales (por ejemplo, el almacenamiento en la nube o auditorías). Exige a estas partes que se garantice la confidencialidad de los datos personales. Si los datos se procesan fuera de la UE (por ejemplo, en los Estados Unidos), se utilizan los contratos modelo prescritos por la Comisión Europea (cláusulas contractuales estándar). Esto significa que sus proveedores no podrán utilizar la información tratada para sus propios fines y que podrán transferir datos personales fuera de la Unión Europea, siempre y cuando se cuente con un nivel de protección adecuado.

País y/o empresa	EU	EQ	EU-US
Snappet BV (Países Bajos)	Sí		
Google Analytics			Sí

EU: País del Espacio Económico Europeo

EQ: País con nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea). Puede consultar la lista de países con nivel adecuado de protección en los siguientes enlaces.

- [Sede Electrónica - Agencia Española de Protección de Datos - Preguntas Frecuentes \(sedeagpd.gob.es\)](https://sedeagpd.gob.es/)
- [Adequacy decisions / European Commission \(europa.eu\)](https://european-commission.europa.eu/)

EU-US: Los datos también pueden localizarse en empresas ubicadas en Estados Unidos siempre que estas hayan formalizado los contratos modelo prescritos por la Comisión Europea (cláusulas contractuales estándar) que garanticen un nivel de protección equivalente.

En cualquier otro caso, se recomienda solicitar información sobre las posibles transferencias internacionales de datos y las garantías de su licitud, en particular sobre las que necesitan autorización por parte de la Agencia Española de Protección de Datos.

9.5 Observaciones

Snappet es un desarrollador de aplicaciones informáticas sobre contenidos educativos, cuyo objetivo principal es el de mejorar la calidad de la educación primaria, de niños menores de catorce años, mediante una solución basada en la enseñanza a través de tabletas. En este contexto, *Snappet* suscribe acuerdos con centros de enseñanza para suministrarles tabletas y hardware afín que incorpora contenidos educativos desarrollados por *Snappet*. Adicionalmente, a través de sus instructores, presta asesoramiento al profesorado de los centros educativos sobre el uso y posibilidades de explotación de las herramientas educativas.

Snappet incluye documentación e información en su web al respecto de la protección de datos y requisitos técnicos.

En toda esta documentación el Colegio es el **responsable de tratamiento**; representado por la persona de contacto responsable de la solicitud. *Snappet España S.L.*, es el **encargado del tratamiento**.

También incluye modelos de los documentos que conforman el Acuerdo entre El Colegio y *Snappet España, S.L.* que incluyen:

- *Acuerdo de uso de contenidos, plataforma y dispositivos electrónicos de Snappet*
- *Acuerdo de Tratamiento de Datos de Carácter Personal*

Integraciones

Snappet puede integrarse con *Microsoft 365 Educación*. *Microsoft* aplica las cláusulas contractuales estándar como base para la transferencia de datos para sus servicios en línea para educación, además de ubicar sus servicios y datos en centros de datos situados en la Unión Europea.

9.6 Prueba de la aplicación

Se considera conveniente poner a prueba la aplicación de forma previa a su definitiva utilización en el centro, realizando la prueba sin introducir datos personales reales de los alumnos ni involucrarlos en su utilización. En esta fase de prueba se debería comprobar la corrección de las informaciones que fueron facilitadas por el responsable de la aplicación.

9.7 Sobre la seguridad de los datos

La responsabilidad del cumplimiento de las medidas de seguridad debe entenderse siempre compartida entre los diferentes actores intervinientes (responsable de la aplicación, centro educativo y usuarios), debiendo en todo caso el responsable de la aplicación facilitar las medidas técnicas adecuadas para garantizar la seguridad de los datos tratados, y el centro aplicarlas o utilizarlas correctamente, además de implementar las medidas organizativas apropiadas.

Así, por ejemplo, la aplicación debe proveer mecanismos que permitan la realización de copias de seguridad o la descarga de los datos, de tal forma que el centro pueda cumplir con las obligaciones que le son exigibles al respecto, introduciendo en su política de seguridad la realización de copias de seguridad de los datos tratados mediante estas aplicaciones, y realizando efectivamente la realización de dichas copias.

La responsabilidad de las medidas de identificación de usuarios también es compartida. Por un lado, la aplicación debe implementar un mecanismo de autenticación que permita la identificación inequívoca y personalizada de los usuarios, recomendándose que este mecanismo consista en códigos de usuario y contraseñas, evitando la identificación de menores mediante datos biométricos (reconocimiento facial o huella dactilar).

Si se utilizan contraseñas, el centro debe incluir en su política el cambio periódico de las mismas, por lo que las aplicaciones que se vayan a utilizar deben incluir mecanismos para permitir dichos cambios. A los usuarios les corresponde la obligación de utilizar contraseñas fuertes y custodiarlas sin desvelarlas a terceros.

10 Historial de versiones

25 de marzo de 2022

Incluida la aplicación *Microsoft Visio* como alternativa a aplicaciones específicas de mapas conceptuales.

18 de noviembre de 2021

Actualizada la sección *Introducción* para recoger la normativa vigente relacionada con protección de datos personales.

Añadida la sección *Aplicaciones externas VS institucionales*.

Actualizada la sección *Mensajería instantánea* para recoger que ya no es necesaria una cuenta de *Microsoft* para acceder a una reunión de *Teams* como invitado.

Añadida la sección *Sobre la ubicación de los datos* para abordar la invalidación del Escudo de Privacidad y la nueva figura de las Cláusulas Contractuales Tipo aprobadas por la Comisión Europea el 4 de junio del 2021.

Incluida la aplicación *Flipgrid* en la sección *Apps móviles*.

Incluida la aplicación *Microsoft Whiteboard* como alternativa a aplicaciones específicas de mapas conceptuales.

Actualizada la sección *Correo electrónico* para reflejar el avance en el uso del correo institucional de Educastur y el posible uso personal de este.

Actualizada la *Plantilla Evaluación de aplicación que almacena datos en nube*.

Actualizada la evaluación de la aplicación *Additio* y añadida la evaluación de la aplicación *Snappet*.

20 de septiembre de 2018

Actualizada la sección *Herramientas de almacenamiento en nube* para recoger la disponibilidad del servicio de *Microsoft Stream* dentro de la plataforma institucional de *Microsoft 365* y la recomendación de sustituir *YouTube* como almacenamiento de vídeos.

18 de mayo de 2018

Primera versión.