ÍNDICE

1. INTRODUCCIÓN

2. DESARROLLO DEL ESTUDIO

3. CONCLUSIONES

   3.1. TIPOS DE APLICACIONES MÓVILES (APPs) UTILIZADAS EN EL ENTORNO EDUCATIVO

   3.2. UTILIZACIÓN DE SISTEMAS DE ALMACENAMIENTO EN NUBE

   3.3. UTILIZACIÓN DE REDES SOCIALES

   3.4. UTILIZACIÓN DE CORREOS ELECTRONICOS DISTINTOS DE LA MENSAJERÍA DE LA PLATAFORMA EDUCATIVA DEL CENTRO

   3.5. OTROS ASPECTOS

4. DECÁLOGO DE RECOMENDACIONES

5. ORIENTACIONES PARA LA EVALUACIÓN DE APLICACIONES

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

La irrupción de las nuevas tecnologías en las aulas producida en los últimos años no ha tenido precedentes, lo que unido a la especial vulnerabilidad de los menores y el gran volumen de datos personales susceptible de tratamientos (8,1 millones de estudiantes no universitarios en España según datos del Ministerio de Educación), llevó a la Agencia Española de Protección de Datos a la realización de una inspección sectorial de oficio sobre servicios de cloud computing en el sector educativo en el año 2015.

Como seguimiento de las recomendaciones recogidas en la referida inspección, esta Agencia ha realizado una iniciativa encaminada a detectar las posibles implicaciones de protección de datos derivadas de la utilización, por parte de los docentes y alumnos, de aplicaciones con almacenamiento de datos en nube, distintas de las plataformas educativas contratadas por los centros.

Esta iniciativa tiene su origen en las conclusiones alcanzadas en las actuaciones preventivas mencionadas, en las cuales se detectó:

- la utilización de diversas aplicaciones informáticas instaladas generalmente en los dispositivos móviles de profesores y alumnos, que podían registrar datos de carácter personal, incluidas imágenes y calificaciones,
- y la utilización de servicios o herramientas de almacenamiento en nube de documentos y ficheros en general, también al margen de las plataformas educativas de los centros, para compartir información entre alumnos, entre profesores, o entre profesores y alumnos.

Durante el año 2016, la Agencia celebró reuniones con las Asociaciones de centros educativos, solicitando su colaboración para la puesta en marcha de un cuestionario on-line al objeto de recabar información de los centros sobre la utilización de este tipo de aplicaciones y herramientas.

Los resultados del presente estudio no constituyen una guía de aplicaciones para educación, sino una guía sobre las implicaciones que dichas aplicaciones pueden tener para la protección de los datos personales. Se detalla un decálogo de conclusiones en el apartado cuarto.

2. DESARROLLO DEL ESTUDIO

El cuestionario online recababa información sobre los siguientes aspectos:

- Utilización de aplicaciones para el aula en dispositivos tales como móviles, tabletas o portátiles, tanto por los alumnos a instancias de los profesores, como por los propios profesores.

- Utilización de herramientas de almacenamiento en nube (tipo Dropbox, Google Drive, etc.), tanto por los alumnos a instancias de los profesores, como por los propios profesores.

- Utilización de redes sociales (Facebook, Instagram, etc.), para trabajos colaborativos u otro tipo de trabajos en el aula.

- Utilización de correo electrónico para el intercambio de información entre alumnos, padres y profesores, distinto de la mensajería propia de la plataforma educativa.

- Existencia en los centros de normas internas y procedimientos con relación al uso de estas aplicaciones.

Una vez redactado el cuestionario y consensuado con las **Asociaciones de Centros Educativos**, se solicitó su colaboración para su puesta en conocimiento por parte de los Centros.

3. CONCLUSIONES

Del análisis de las respuestas que han sido aportadas se desprenden las siguientes consideraciones, separadas para los cuatros bloques de aplicaciones que aparecen en el estudio: apps móviles, herramientas de almacenamiento en nube, redes sociales y correo electrónico:

3.1 TIPOS DE APLICACIONES MÓVILES (APPs) UTILIZADAS EN EL ENTORNO EDUCATIVO

De la información obtenida se desprende que existen multitud de Apps para el entorno educativo, instalables en dispositivos móviles tipo tableta o teléfono móvil inteligente, aunque la mayoría ofrecen también la posibilidad de utilización desde un ordenador personal con navegador de internet.

La mayoría de los Centros permite la utilización de estas aplicaciones, declarando en muchos casos que mediante ellas se almacenan datos personales, si bien normalmente limitados al nombre y apellidos de los alumnos. También se almacenan trabajos realizados y, en menor medida, calificaciones. Asimismo, se ha declarado el almacenamiento de fotos, videos y grabaciones de voz.

Las aplicaciones utilizadas responden a una gran variedad, que se pueden clasificar en los siguientes tipos según su funcionalidad (se mencionan entre paréntesis algunas aplicaciones a modo de ejemplo):

1. Aplicaciones que implementan cuadernos de notas, agendas y organizador de clases para los docentes (IDOCEO, ADDITIO, TEACHER AIDE).

2. Aplicaciones puramente destinadas a ofrecer materiales didácticos atrayentes para los alumnos y de utilidad para los profesores, de diferentes materias como matemáticas, ciencias, (DIDAKIDS), incluyendo gamificación (CLASSCRAFT, KAHOOT), etc.

3. Aplicaciones para la creación de hilos de discusión y debate, compartición de mapas mentales, conceptuales y esquemas (MINDOMO).

4. Aplicaciones para la elaboración de presentaciones (PREZI, TED).

5. Aplicaciones que facilitan la comunicación entre profesores, alumnos y familias. Si bien esta funcionalidad se suele incorporar en las plataformas educativas, existen apps con esta finalidad exclusiva. También, dentro de este tipo de aplicaciones, señalar que se ha detectado la utilización de mensajería WHATSAPP en los entornos educativos.

6. Creación y compartición de vídeos. (ANIMOTO, MOVIE MAKER). Edición y compartición de fotografías y vídeos (PicCOLLAGE).

7. Aplicaciones que convierten tabletas en pizarras digitales para compartir información en tiempo real (ACTIVEINSPIRE).

8. Apps para el acceso desde el terminal móvil a plataformas de aprendizaje (MOODLE, LMS WORDPRESS, SCHOOLOGY), para la compartición de recursos de estudio, realización de trabajos en grupo, etc. También existen redes sociales educativas con funciones de plataformas de aprendizaje (CLASSROOM, EDMODO).

Dejando a un lado las plataformas educativas y de aprendizaje, que no eran objeto de este estudio, las aplicaciones que más datos personales de los alumnos pueden llegar a tratar son los cuadernos de notas de los docentes, que mantienen el progreso y las calificaciones de los alumnos, sin olvidar que aunque la mayoría del resto de aplicaciones no recopilan datos personales más allá de los básicos de usuario, cualquier aplicación que incluya la identificación del alumno puede llevar a la elaboración de perfiles según las funcionalidades y la tipología de los datos recopilados.

Con los hábitos de navegación de un usuario, los datos de otros usuarios con los que contacta y su comportamiento educacional se podrían crear perfiles, tratamientos en ocasiones escudados en la mejora del funcionamiento del servicio. Los usuarios se pueden clasificar fácilmente según su actividad (las acciones que realizan) o incluso el tiempo que tardan en realizarlas.

Hay que tener en cuenta que las aplicaciones instalables en dispositivos móviles inteligentes son capaces de acceder a gran cantidad de datos de carácter personal almacenados en el propio dispositivo, tales como el número de identificación del terminal, agenda de contactos, imágenes o vídeos. Además, estas aplicaciones pueden acceder a los sensores del dispositivo, y obtener la ubicación geográfica, capturar fotos, vídeo o sonido a través de ellos.

Las Autoridades europeas de protección de datos aprobaron conjuntamente en marzo de 2013 un dictamen sobre aplicaciones móviles para dispositivos móviles inteligentes. Dicho dictamen puede consultarse aquí.

3.2 UTILIZACIÓN DE SISTEMAS DE ALMACENAMIENTO EN NUBE

De las respuestas se desprende que utilizan en gran medida las herramientas de almacenamiento en nube siguientes: DROPBOX, Google DRIVE e iCLOUD.

Son utilizadas tanto por los profesores como por los alumnos con la finalidad fundamental de compartir documentos, normalmente apuntes de clase y materiales didácticos en general, así como trabajos de los alumnos. En algunas ocasiones se ha declarado la utilización de estas herramientas para almacenar datos personales tales como listas de asistencia, calificaciones, fotos y vídeos.

3.3 UTILIZACIÓN DE REDES SOCIALES

De las respuestas se desprende que se utilizan, aunque moderadamente, redes sociales en los Centros. Facebook es la más mencionada, seguida de Twitter e Instagram.

Son utilizadas tanto por los profesores como por los alumnos, generando una mayor cohesión del grupo de alumnos. Se utilizan fundamentalmente como canal de comunicación y como medio de compartir información (fotos, información de eventos, etc.)

3.4 UTILIZACIÓN DE CORREOS ELECTRONICOS DISTINTOS DE LA MENSAJERÍA DE LA PLATAFORMA EDUCATIVA DEL CENTRO

De las respuestas obtenidas se evidencia que el sistema de mensajería o correo facilitado por la plataforma educativa no es el único sistema utilizado por los centros, utilizándose también otros correos electrónicos, mayoritariamente correos corporativos independientes de la plataforma. Solo un número reducido de Centros utiliza exclusivamente la mensajería de la plataforma.

También se ha declarado la utilización de la aplicación Whatsapp para comunicaciones en grupos.

3.5 OTROS ASPECTOS

Algunos de los Centros participantes en el estudio han declarado haber establecido normas internas regulando el uso de las aplicaciones, así como procedimientos para autorizar su uso, realizando evaluaciones de seguridad de las aplicaciones.

4. DECÁLOGO DE RECOMENDACIONES

1. Los Centros Educativos deben observar la debida diligencia con los tratamientos de datos personales que se efectúen en el Centro, incluyendo los que se producen como consecuencia de la llegada de las tecnologías a las aulas, velando por que se reúnan las garantías para el cumplimiento de lo dispuesto en la normativa de protección de datos.

2. Algunas aplicaciones utilizadas no ofrecen suficiente información para valorar su adecuación a la normativa. Por ejemplo, en materia de seguridad, sobre la ubicación de los datos, el periodo de retención de los mismos, ni los responsables de los tratamientos. En ocasiones no incluyen información ni tan siquiera sobre las finalidades de los tratamientos, detectándose falta de transparencia y la posibilidad de prácticas de retención de datos opacas.

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.

Por ello, deben utilizarse únicamente aquellas aplicaciones que ofrezcan información claramente definida sobre los tratamientos efectuados, las finalidades de los mismos y sus responsables, así como sobre la ubicación de los datos, el periodo de retención, y las garantías con relación a su seguridad.

3. Las aplicaciones educativas, que pueden ser de gran utilidad para el aprendizaje así como para la organización de las aulas, deben estar incluidas en la política de seguridad de los centros educativos, debiendo los profesores solicitar, previamente a su utilización, la autorización del centro.

Deben establecerse procedimientos que obliguen a solicitar la autorización del Centro para el uso de estas aplicaciones. Una solicitud de autorización conllevará la evaluación de la aplicación desde el punto de vista de la seguridad de la información y la consiguiente autorización o denegación por parte del Centro.

Los tratamientos de datos personales mediante apps deben de incluirse en la política de seguridad con las mismas garantías que cualquier otro tratamiento.

En el apartado 5 del presente informe se pueden consultar orientaciones para la realización de la evaluación de las aplicaciones.

4. Los centros deben informar a los padres o tutores del comienzo de la utilización de la tecnología en las aulas, así como de las Apps que traten datos personales de los alumnos y su funcionalidad.

En particular, se considera que el usuario y las familias deben ser informadas de la utilización de sistemas de almacenamiento en nube.

Según el Reglamento General de Protección de Datos, aplicable el 25 de mayo de 2018,la información ofrecida deberá ser concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en especial la dirigida a los menores. Los Centros deberían de ir adaptando la información que ofrecen a esta nueva normativa.

5. Las aplicaciones que se utilicen deben permitir el control, por parte de los tutores o profesores, de los contenidos subidos por los menores, en especial de los contenidos multimedia (fotos, vídeos y grabaciones de voz de los alumnos).

6. Debe guardarse especial cuidado con los tratamientos de datos personales que sean facilitados por terceros sin mediación del titular de los datos, y en concreto, con la publicación de fotografías o vídeos de alumnos facilitados por otros alumnos o profesores.

7. Deben establecerse programas informativos de concienciación orientados hacia la protección de los datos personales, dirigidos a profesores y alumnos, sobre la importancia del uso correcto de aplicaciones.

Entre las informaciones y normas internas que deberían de dictarse se indican, a modo de orientación práctica, las siguientes:

- Los usuarios deben tener especial cuidado al publicar imágenes y vídeos mediante apps y herramientas en nube para no poner en riesgo la intimidad de otras personas.
- Se recomienda leer la información sobre el servicio (política de privacidad y condiciones de uso) antes de empezar a utilizarlo.
- Al utilizar redes sociales se recomienda configurar las opciones de privacidad en el perfil de usuario para permitir el acceso a la información publicada a un grupo conocido y previamente definido de usuarios.
- Al facilitar datos en cualquier ámbito (en cualquier tipo de aplicación, en el registro de usuarios, en los contenidos) evitar incorporar datos del domicilio de los menores y otros datos personales que puedan poner en peligro su seguridad. Debe recomendarse no atender la demanda que puedan tener las aplicaciones para recabar datos personales, que pueda llevar al tratamiento de datos excesivos.

- Las contraseñas deben ser robustas, evitando las que sean fáciles de adivinar por otras personas, con suficientes caracteres y compuestas por mayúsculas, minúsculas, números y caracteres especiales.

  No se deben de facilitar nunca a otras personas.

8. Al utilizar sistemas de almacenamiento de documentos en nube tipo Dropbox, iCloud o Google Drive, se debe evitar incluir datos personales sensibles, tales como datos relativos a la salud, contraseñas, datos bancarios, material audiovisual de contenido sensible, etc.

En el marco de la utilización de este tipo de herramientas se recomienda la lectura de la guía de cloud publicada por la Agencia Española de Protección de Datos, accesible en este enlace.

9. Cuando exista en el Centro una plataforma educativa que permita la interacción entre alumnos, y entre estos y los profesores, se aconseja que se prime su utilización para este fin, sin establecer mecanismos de comunicación adicionales.

10. Para los casos de tratamientos especiales de datos personales que puedan suponer un mayor riesgo, tal como el reconocimiento facial de menores de edad, que implica el tratamiento de datos biométricos, el responsable debe obtener el consentimiento expreso de los alumnos (si son mayores de 14 años) o de los padres o tutores (si son menores de 14 años) para aplicar dicho tratamiento a las imágenes con fines de identificación, y asegurarse que esta tecnología se utiliza únicamente para fines concretos especificados y legítimos.

Este límite de edad de 14 años puede sufrir modificaciones con la futura aprobación de la nueva Ley Orgánica de Protección de Datos, en fase de tramitación parlamentaria en el momento en el que se publica este informe (febrero 2018).

5. ORIENTACIONES PARA LA EVALUACIÓN DE APLICACIONES

Para la evaluación de las aplicaciones desde el punto de vista de la protección de los datos personales y la seguridad de la información los Centros pueden seguir las siguientes orientaciones:

Sobre la información ofrecida por los responsables de la aplicación:

Se debe comprobar si el responsable de la aplicación informa claramente de los siguientes

- la identidad y dirección del responsable,
- las finalidades para las que serán utilizados los datos,
- las posibles comunicaciones de datos a terceros y su identidad, así como la finalidad por la que se ceden,
- los derechos que asisten a los titulares de los datos,
- la ubicación de los datos y sus periodos de conservación,
- las medidas de seguridad facilitadas por la aplicación,
- los posibles accesos que realiza la aplicación a los datos personales almacenados en el dispositivo o a sus sensores.

Esta información debería estar fácilmente accesible en la política de seguridad 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.

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 consultar la lista de países con nivel adecuado de protección en el siguiente enlace.

Los datos también pueden localizarse en empresas ubicadas en Estados Unidos siempre que éstas se hayan acogido a los principios del Escudo de Privacidad. Si desea saber si una empresa de Estados Unidos forma parte del Escudo de Privacidad, puede consultar la Lista empresas adheridas.

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.

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 de contraseñas robustas y custodiarlas sin desvelarlas a terceros.

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.

Documentación de la evaluación:

Se recomienda documentar las evaluaciones realizadas dejando constancia de los aspectos que han sido analizados y de los resultados obtenidos.

ORIENTACIONES PARA CENTROS EDUCATIVOS AEPD

INFORME SOBRE LA UTILIZACIÓN POR PARTE DE PROFESORES Y ALUMNOS DE APLICACIONES QUE ALMACENAN DATOS EN NUBE CON SISTEMAS AJENOS A LAS PLATAFORMAS EDUCATIVAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS