UTILIZACIÓN DE APLICACIONES AJENAS A LAS DE LA COMUNIDAD DE MADRID

Del uso cada vez más extendido de las nuevas tecnologías en las aulas y de la entrada en vigor de una normativa sobre protección de datos personales más estricta para garantizar los derechos y libertades de las personas nace la necesidad de adoptar en los centros educativos medidas de seguridad y de privacidad más robustas que las que venían aplicándose hasta ahora.

Esto significa que, de la misma manera que para seguir una dieta saludable elegimos alimentos con altas propiedades nutritivas frente a otros que pueden ser perjudiciales o que, sin serlo, es conveniente tomarlos con precaución, debemos seguir estos mismos criterios cuando vamos a elegir las herramientas más adecuadas y seguras para impartir las enseñanzas en nuestro centro educativo.

Especialmente importante es prestar atención a esta cuestión con motivo de la necesidad de utilizar la modalidad a distancia o en línea tras el confinamiento de la población en sus domicilios, que ha impedido continuar con el habitual sistema educativo presencial. Sin embargo, la vuelta a la normalidad no significa que este sistema tenga que desaparecer; por el contrario, estas modalidades probablemente permanecerán como complemento y, en muchos casos, como sustitutos de procedimientos tradicionales para impartir la docencia.

Los centros educativos deben observar la debida diligencia con los tratamientos de datos personales, pero especialmente cuando se producen como consecuencia del uso de las nuevas tecnologías, que pueden poner en riesgo con mayor facilidad la privacidad y confidencialidad de los datos, sobre todo si no se conoce en profundidad la política de seguridad de la información y de privacidad de los datos personales de la organización a la que pertenecen, cuyo contenido debe darse a conocer por esta a sus empleados.

La **Agencia Española de Protección de Datos** (AEPD), advierte sobre los riesgos de utilizar aplicaciones que no ofrezcan la información suficiente para poder valorar su adecuación a la normativa[1].

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,
- sobre el periodo de retención de estos,
- ni sobre 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 pueden contener la elaboración, por parte de los responsables de las aplicaciones, de perfiles de aprendizaje, preferencias o comportamiento, incluyendo los de los menores de edad.

Las aplicaciones que más datos personales de los alumnos pueden llegar a tratar son los cuadernos del profesor, que mantienen el progreso y las calificaciones de los alumnos, es decir, son datos subjetivos y por ello de carácter sensible además de ser confidenciales porque son fruto de la política educativa de la organización, sin olvidar que aunque la mayoría de aplicaciones no recopilan datos personales más allá de los básicos u objetivos del usuario, cualquier aplicación

[1] Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas

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 va agregando información sobre los individuos y sobre los grupos sociales a los que pertenecen, que permiten 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.

Por ello, **deben utilizarse únicamente aquellas aplicaciones que ofrezcan información claramente definida sobre**

- los tratamientos efectuados,
- las finalidades de estos y sus responsables,
- así como sobre la ubicación de los datos,
- el periodo de retención, y
- las garantías con relación a su seguridad.

Sin embargo, a pesar de que hayamos podido elegir las que garanticen el cumplimiento de la normativa de seguridad y de privacidad de la información, las empresas prestadoras de los servicios no se hacen responsables del tipo y de la cantidad de datos personales que los usuarios de las aplicaciones alojan en ellas, razón por la cual deben diseñarse procedimientos para utilizar los datos que sean estrictamente indispensables y lo más objetivos posible, como datos identificativos para el acceso, evitando escrupulosamente introducir datos subjetivos, como valoraciones de conocimientos, conductas u opiniones, o cualquier otra información de carácter sensible o confidencial como pueden ser los datos de salud.

Debemos tener presente que los diferentes centros directivos o **direcciones generales** de la Consejería **son responsables del tratamiento de los datos personales en su respectivo ámbito de actividad y les corresponde la gestión, coordinación y dirección del tratamiento de los datos, así como la determinación de los fines y medios para garantizar el cumplimiento de la normativa en materia de protección de datos**[2].

Aunque el director de un centro educativo público ejerce sus competencias de acuerdo con la autonomía de gestión que le otorga la Ley Orgánica de Educación, no es responsable del tratamiento de datos de carácter personal, dado que el centro público no es un órgano directivo con capacidad de decisión sobre el tratamiento de datos personales, sino que forma parte de la estructura orgánica de la Consejería, sigue sus directrices y ejecuta las políticas de privacidad que le son encomendadas**.**

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 relativa a los centros educativos**, **debiendo estos solicitar, previamente a su utilización, la autorización del responsable del tratamiento**. En el caso de un centro privado o concertado el responsable es el propio centro, pero en el caso de un centro público, como se ha indicado más arriba, el responsable es la Dirección General competente.

Debe establecerse un procedimiento claro para solicitar por parte del Centro la autorización previa del responsable antes del 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 privacidad de los datos personales** y la consiguiente autorización o denegación por parte del responsable. Tras la autorización el centro podrá aprobar su puesta en funcionamiento y su

[2] Disposición Adicional Primera del DECRETO 288/2019, de 12 noviembre, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Educación y Juventud.

incorporación a la Programación General Anual (PGA), con el detalle del uso y de los datos personales que se verán afectados. La PGA deberá estar accesible a la comunidad educativa del centro para su consulta.

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 informe se pueden consultar orientaciones para la realización de la evaluación de las aplicaciones.

Los centros deben informar a los padres o tutores del comienzo de la utilización detallada de la aplicaciones y plataformas en las aulas, así como de las *Apps* que traten datos personales de los alumnos y su funcionalidad. En particular, el usuario y las familias deben ser informados de la utilización de sistemas de almacenamiento en nube.

Según el Reglamento General de Protección de Datos, 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 ir adaptando la información que ofrecen a esta nueva normativa.

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), pero paralelamente, debe concienciarse al alumnado de la importancia de esmerarse en el cuidado la identidad digital personal, pues supone la responsabilidad de diseñar la propia imagen social, que será nuestra carta de presentación pasada, presente y futura.

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, debiendo advertirles de que no pueden publicarse o difundirse sin el consentimiento de todos aquellos que aparecen en ese contenido audiovisual. Véanse los modelos de consentimiento oficial publicados en la página web de esta Delegación de Protección de Datos.

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, sobre todo al inicio del curso escolar, haciendo hincapié en ello durante las sesiones docentes que tengan relación con el tratamiento de datos personales.

Entre las informaciones y normas internas que deberían dictarse e incluirse en el Reglamento de Régimen Interior 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, independientemente del tipo de aplicación, sea esta corporativa o no.
- Se recomienda **leer la información sobre el servicio** (política de privacidad y condiciones de uso) **antes de empezar a utilizarlo y siempre evitar introducir información de carácter confidencial.**
- Antes de utilizar las **redes sociales** se recomienda informar y formar a los alumnos sobre el procedimiento para configurar las opciones de privacidad en el perfil de usuario, con el fin de 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) se debe evitar incorporar datos como el 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.

Si bien no hay nada que objetar sobre el **uso privado** de sistemas de almacenamiento de documentos en nube tipo Dropbox, iCloud o Google Drive, **se debe evitar utilizarlos para el tratamiento de información de carácter profesional y, por lo tanto, confidencial**, como es la relación entre alumno y profesor. Para esta actividad los centros tienen a su disposición las herramientas corporativas facilitadas por el responsable. En consecuencia, nunca se debería introducir datos personales sensibles, tales como los relativos a la salud, contraseñas, datos bancarios, material audiovisual de contenido sensible, observaciones sobre comportamientos, rendimiento escolar, etc., en nubes ajenas a la organización, como se detalla en el aparado siguiente.

En el marco de la utilización de este tipo de herramientas se recomienda la lectura de la guía de "Cloud" publicada por la AEPD.

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 que demuestren la proporcionalidad de la medida.

Entre las recomendaciones de la AEPD se insiste, además, en que ***"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".***

PLATAFORMA EDUCATIVA DE LA COMUNIDAD DE MADRID

En el caso de la Comunidad de Madrid, la Consejería de Educación y Juventud, como responsable de proporcionar las herramientas necesarias para que los centros educativos puedan proporcionar una enseñanza de calidad que incluya el uso de las tecnologías de la información, desde hace muchos años pone a su disposición la plataforma EducaMadrid, un conjunto de servicios públicos y gratuitos para centros educativos, profesores, alumnado y familias, dotado de las adecuadas medidas de seguridad y conforme con la normativa de protección de datos de carácter personal.

Cuando el centro educativo haga uso de aplicaciones y herramientas externas a las institucionales de la Consejería de Educación y Juventud hay que saber que, además de las acciones previas recogidas en las recomendaciones de la AEPD, deberá tenerse en cuenta lo siguiente:

- Según el Reglamento General de Protección de Datos, el responsable del tratamiento es quien determina los fines y medios del tratamiento. En relación con el tratamiento de datos en los centros educativos, el responsable del tratamiento es el propio centro cuando este es privado o privado concertado y en los centros educativos públicos, el responsable es la Consejería competente en materia de educación.
- La Disposición Adicional Primera del Decreto de estructura de la Consejería de Educación y Juventud dispone lo siguiente: "***Los diferentes centros directivos de la consejería son responsables del tratamiento de los datos personales en su respectivo ámbito de actividad y les corresponde la gestión, coordinación y dirección del tratamiento de los datos, así como la determinación de los fines y medios para garantizar el cumplimiento de la normativa en materia de protección de datos***.".
- Aunque **el director de un centro educativo** público ejerce sus competencias de acuerdo con la autonomía de gestión que le otorga la Ley Orgánica de Educación, **no es responsable del tratamiento de datos de carácter personal, dado que el centro público**

no es un órgano directivo con capacidad de decisión sobre el tratamiento de datos personales, sino que forma parte de la estructura orgánica de la Consejería, sigue sus directrices y ejecuta las políticas de privacidad que le son encomendadas.

- El uso de aplicaciones educativas externas sólo está justificado cuando no se hayan puesto a disposición de los centros los medios o herramientas adecuadas y equivalentes y **requerirá la autorización del centro educativo en el caso de centros privados o concertados y, en el caso de centros educativos públicos, de la dirección general de la Consejería competente en materia de educación**[3], que deberá establecer un procedimiento, en aras de la seguridad jurídica, que impida el uso de aquellas que no hayan sido aprobadas expresamente. Para garantizar que se van a utilizar cumpliendo con todos los requisitos que afectan a la seguridad de los datos, con anterioridad a su uso se habrá de realizar una **evaluación de cada aplicación desde el punto de vista de la seguridad de la información**. Esto exige el diseño y restricciones sobre la cantidad y tipo de datos que van a ser incorporados en las aplicaciones, que tendrá en cuenta en primer lugar la privacidad de los datos personales, e incluirá valorar la necesidad de disociar o anonimizar la información, especialmente cuando exista cesión de datos a terceros o transferencias internacionales de datos. De todo ello deberá existir constancia documental.

- Estas evaluaciones y la decisión final sobre el uso de las aplicaciones o plataformas educativas deben ser validadas por el responsable del tratamiento de datos personales, la Consejería de Educación y Juventud a través de las correspondientes direcciones generales, y deben someterse a la supervisión por la Delegación de protección de datos de la Consejería, que comprobará su adecuación a la normativa aplicable.

- Una vez que el uso de una aplicación haya sido autorizado por el centro educativo, éste deberá incluir **en la Programación General Anual del curso** el uso justificado de las correspondientes plataformas o aplicaciones externas, previa comprobación de que cumplen con la política de privacidad exigida por el Reglamento (UE) 2016/679 de Protección de Datos. En ella se incorporará información clara sobre los tratamientos efectuados, sus responsables, sus finalidades, la ubicación de los datos, el periodo de conservación y las garantías sobre su seguridad. Dicha información deberá darse a conocer a las familias y los alumnos mayores de 14 años a través de su publicación en la página web del centro y de cualquier otro medio que asegure la obligación de informar sobre las finalidades adicionales del uso de dichas herramientas. 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.

- Es conveniente que las familias consulten la PGA para tener información adecuada, pues una vez aprobado su uso, **existe la obligación de suscribir un contrato o cualquier otra figura jurídica que vincule al responsable con el encargado de tratamiento, es decir, las empresas prestadoras del servicio, que requiere recabar el consentimiento de las familias** para que dichas empresas puedan tratar sus datos personales.

- No obstante, cuando las empresas prestadoras del servicio son multinacionales o poseen un gran volumen de negocio, el centro educativo no puede suscribir por sí mismo un contrato o acuerdo, sino que debe aceptar las condiciones de uso de las aplicaciones o plataformas que aquellas hayan establecido, lo que contradice el requisito establecido por el Reglamento de Protección de Datos según el cual es el responsable quien debe imponer las condiciones para el tratamiento de los datos por el encargado

  Por esta razón la Dirección General de Bilingüismo y Calidad de la Enseñanza, como responsable según el actual marco competencial, deberá validar el uso de las plataformas o

[3] En la actualidad, la Dirección General de Bilingüismo y Calidad de la Enseñanza, por ser competente en fijar las directrices de uso de las aplicaciones y plataformas educativas.

aplicaciones ajenas por parte de los centros, y **deberá suscribirse un acuerdo o contrato donde figure dicha Dirección General como responsable del tratamiento y como encargado de este la empresa prestadora, estableciendo conjuntamente las condiciones del tratamiento por parte del centro educativo**. Una vez suscrito el acuerdo, las Dirección General de Educación Infantil y Primaria y la Dirección General de Educación Secundaria, Formación Profesional y Régimen Especial serán responsables, en función de las competencias atribuidas por el Decreto de estructura de la Consejería[4], del cumplimiento de lo acordado por parte de los centros educativos.

En resumen,

- El uso de aplicaciones educativas externas por el centro debe adecuarse a la normativa sobre seguridad y sobre protección de datos personales. Es necesario que los centros públicos de la Comunidad de Madrid se aseguren de ello y recaben la autorización del responsable del tratamiento, es decir, la Dirección General de Bilingüismo y Calidad de la Enseñanza, con el asesoramiento del Delegado de Protección de Datos. Además, es obligatoria la existencia de un contrato de encargo del tratamiento que vincule a la Consejería y al encargado del tratamiento.
- Cuando en la aplicación se vayan a incorporar datos personales, el centro deberá recabar el **consentimiento[5] de las familias y de los alumnos para el tratamiento de los datos por el encargado del tratamiento, es decir la empresa prestadora del servicio.**
- Hay que tener en cuenta que cuando la aplicación vaya a utilizarse dentro del centro educativo en dispositivos móviles ajenos a la Consejería (por ejemplo: ordenador portátil, tableta o teléfono móvil propiedad del profesor), estos dispositivos se están integrando en la red de la corporación. Por lo tanto, si se permite su uso, debe establecerse una política reguladora del ámbito al que pueda afectar, es decir, si se va a utilizar por los profesores para la gestión de sus tareas o si también se van a manejar en las aulas por profesores y alumnos.
- Si la organización decide permitir la utilización de dispositivos privados, es necesario que se establezcan unas directrices que regulen la implementación del principio *"Bring your own device"* (BOYD), estableciendo reglas precisas sobre los derechos de control y acceso, la privacidad de los trabajadores y la protección de datos en la corporación, evitando dejar que los centros educativos decidan sobre estas cuestiones que transcienden la mera actualización tecnológica, porque incide directamente en la seguridad y la confidencialidad de la información de la organización en general y, particularmente, en la privacidad de los datos personales, incluidos los de carácter sensible, de los miembros de la comunidad educativa. Recomendamos la lectura del informe elaborado por el INTEF al respecto.

Madrid, abril de 2020

DELEGACIÓN DE PROTECCIÓN DE DATOS

Firmado electrónicamente por: David Lleras Iglesias

Ubicación: Madrid
Fecha: 2020.05.05 20:24:09 +02'00'

[4] Decreto 288/2019, de 12 noviembre, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Educación y Juventud. Art. 8.1.k), l) y n) y Art. 10.1.i), p) y q)
[5] Ver los modelos de consentimiento oficial publicados en la página web de la Delegación