

## **RECOMENDACIÓN 2019-002: USO DE APLICACIONES EXTERNAS POR PARTE DE LOS CENTROS EDUCATIVOS QUE IMPLICAN EL TRATAMIENTO DE DATOS PERSONALES**

¿Qué es un dato de carácter personal?.....	1
¿Qué es un tratamiento de datos personales?.....	1
¿ Hay que tener un cuidado especial con los datos de los menores?.....	2
¿Quién es el responsable de los datos personales que se tratan en los centros?.....	2
¿Qué es un “encargado del tratamiento”?.....	2
¿Es posible utilizar aplicaciones de terceros para tratar datos personales de los centros?.....	3
Si se utilizan aplicaciones de terceros, ¿hay alguna diferencia entre que los datos estén en la “nube” o en un dispositivo propiedad del centro?.....	3
CASOS PRÁCTICOS: Uso de herramientas en la «nube» para la realización de actividades docentes.....	4
CASOS PRÁCTICOS: Uso de herramientas de correo electrónico y mensajería instantánea.....	6
CASOS PRÁCTICOS: Uso de cuadernos de notas y seguimiento de la actividad docente.....	7

### **¿Qué es un dato de carácter personal?**

Cualquier información que pueda ser relacionada con una persona física identificada o identificable. Eso incluye, entre otros, además de los datos puramente identificativos (nombre, apellidos, DNI...), las calificaciones, resultados de evaluaciones o trabajos, datos de salud (patologías, minusvalías o grados de minusvalía, resultados de evaluaciones psicológicas...), imagen o voz (grabaciones de video y audio, fotos...) de las personas.

### **¿Qué es un tratamiento de datos personales?**

Cualquier operación que se realice sobre datos personales o conjuntos de datos personales, independientemente de que se haga por medio de procedimientos automatizados o manuales. En consecuencia, su almacenamiento, difusión o publicación, entre otros, tienen la consideración de tratamientos de datos y se les tiene que aplicar la normativa vigente en la materia.

### **¿ Hay que tener un cuidado especial con los datos de los menores?**

Los y las menores merecen una protección específica de sus datos personales, dado que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos relativos al tratamiento de datos personales.

### **¿Quién es el responsable de los datos personales que se tratan en los centros?**

El responsable de los datos personales, según lo previsto en el artículo 4 del RGPD, es la persona física o jurídica, autoridad pública, servicio u otro organismo que, por él mismo o junto con otros, determine las finalidades y medios del tratamiento. A todos los efectos, la Conselleria de Educación, Cultura y Deporte será responsable de los datos del personal y alumnado del centro y dará las instrucciones oportunas para el tratamiento de las mismas por parte de sus trabajadores y trabajadoras. Estos datos son los que se alojan en ITACA y son accedidos y tratados por su personal en el ejercicio de sus funciones.

Sin embargo, pueden existir tratamientos de datos personales sobre los cuales el centro decida cómo hacerlos y para qué hacerlos (grabación de actividades, difusión de información, redes sociales...). En estos casos, la responsabilidad será del centro y su ejercicio recaerá en la dirección de este, conforme a las competencias establecidas en el artículo 132 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

Cualquier tratamiento de datos personales de las y los estudiantes, del personal o de padres y madres, con finalidad distinta del uso exclusivamente personal o doméstico, debe tener una habilitación legal que, con carácter general, puede ser el cumplimiento de una obligación legal, el desarrollo de una misión en interés público o del ejercicio de competencias previstas en una ley, o el consentimiento de los afectados.

### ¿Qué es un “encargado del tratamiento”?

El encargado del tratamiento es un tercero, empresa u organismo público, que hace un tratamiento de los datos personales por cuenta de su responsable. Por lo tanto, una empresa ajena al centro que proporcione una aplicación que almacene datos del alumnado o que los trate o tenga acceso a los mismos de cualquier otra manera **podría tener la consideración de encargado del tratamiento de los datos personales que son responsabilidad del centro** o de la Conselleria si cumple las condiciones siguientes:

- Que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas de seguridad apropiadas, de forma que el tratamiento sea conforme con los requisitos legales y garantice la protección de los derechos del interesado.
- **Que exista un contrato u otro acto jurídico que vincule al encargado (el tercero) respecto del responsable (el centro)** y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales, las categorías de interesados, los derechos de los afectados y las responsabilidades de cada una de las partes.

La firma de un contrato o una resolución que vincule al encargado debe efectuarla **quien tenga la capacidad legal de representar al responsable** del tratamiento y, preferiblemente, debe constar por escrito. La aceptación mediante un “click” de las condiciones impuestas por una plataforma no reúne, con carácter general, estas condiciones.

### ¿Es posible utilizar aplicaciones de terceros para tratar datos personales de los centros?

Para poder usar aplicaciones de terceros que tratan datos personales que sean responsabilidad del centro o de la Conselleria, hará falta que se cumplan dos condiciones:

- Que si el tercero propietario o autor de la aplicación tiene o puede tener acceso a los datos personales, asuma la condición de encargado de tratamiento y exista el correspondiente contrato entre él y el responsable (Conselleria o centro), o un acto jurídico equivalente.



- Que la aplicació haya sido aprobada para su uso por la Conselleria como dicen tanto la resolución del 28 de junio de 2018 de la Subsecretaria, como la resolución del 5 de julio de 2019 del secretario autonómico de Educación y Formación Profesional.

### **Si se utilizan aplicaciones de terceros, ¿hay alguna diferencia entre que los datos estén en la “nube” o en un dispositivo propiedad del centro?**

Si los datos están en la nube, el tercero que proporciona el servicio siempre tiene acceso a los mismos y, en consecuencia, será imprescindible que obtenga previamente la condición de encargado del tratamiento de los datos personales.

Si los datos están en un dispositivo propio del centro o de la administración educativa, el tercero propietario o autor de la aplicación no necesariamente tiene que tener acceso a los datos.

El Reglamento General de Protección de Datos también establece que los datos personales tendrán que ser tratados de tal manera que se garantice una seguridad adecuada de estos. La Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digitales determina que los organismos públicos tendrán que aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad. El uso de dispositivos personales como puedan ser los ordenadores de uso privado, bien sean portátiles o de sobremesa, *tablets* o teléfonos móviles, puede comprometer la seguridad de los datos personales porque no están sujetos estos dispositivos, a todos los efectos, al cumplimiento de lo que prevé el Esquema Nacional de Seguridad.

### **CASOS PRÁCTICOS: Uso de herramientas en la «nube» para la realización de actividades docentes**

Situación:

- El/la profesor/a accede a la web de una herramienta determinada y establece un grupo de trabajo con un código específico.
- El/la profesor/a entrega este código a su alumnado y da instrucciones para que se registren individualmente en la plataforma, lo cual requiere que los/las estudiantes se identifiquen,



introduciendo sus datos personales y dirección de correo electrónico. Presumiblemente también quedarán identificados por la dirección IP del equipo desde el cual se hace la grabación.

- La inscripción de los/las estudiantes se considera obligatoria por parte del/la profesor/a porque utiliza la plataforma como parte del proceso de educación y evaluación de los/las estudiantes.

La situación descrita, desde la perspectiva de protección de datos personales, implica que el centro sería responsable del tratamiento de los datos de los/las estudiantes con fines educativos y de evaluación y que el propietario de la plataforma sería encargado del tratamiento de esos datos. Esta situación requeriría la firma de un contrato entre el centro y el propietario de la plataforma en los términos previstos al artículo 28.3 del RGPD.

Además, según se establece en la Orden 19/2013, de 3 de diciembre, de la Conselleria de Hacienda y Administración Pública, por la cual se establecen las normas sobre el uso seguro de medios tecnológicos en la Administración de la Generalitat, en su artículo 5, *“Queda prohibido, así mismo, transmitir o alojar información propia de la Administración de la Generalitat en sistemas de información externos, excepto autorización expresa del organismo responsable del tratamiento de la información, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato exprés entre la Administración de la Generalitat y la empresa responsable de la prestación del servicio, incluyendo los acuerdos de nivel de servicio que sean procedentes, el acuerdo de confidencialidad correspondiente y siempre con el análisis previo de los riesgos asociados a tal externalización”* .

Hay que recordar que la finalidad de la formalización del encargo de tratamiento por medio de un contrato o acto jurídico es, entre otros, dejar claro que el propietario de la plataforma no puede utilizar los datos personales del alumnado del centro para ninguna finalidad distinta de la de facilitar la realización de los ejercicios y la evaluación de los/las estudiantes y obligarle a borrar estos datos cuando así se lo indicara el centro o la Conselleria, como responsables del tratamiento. La mayor parte de plataformas que se ofrecen de manera gratuita no contemplan esta posibilidad y consideran que son responsables del tratamiento de todos los datos de los usuarios que se han registrado libremente en su plataforma, de acuerdo con un interés legítimo (artículo 6.1.f del

RGPD), lo cual implica poder decidir sobre las finalidades de las mismas de acuerdo con su propia política de privacidad.

Sin embargo, este tipo de plataformas se podría utilizar, atendiendo exclusivamente a la normativa vigente en materia de protección de datos, si la inscripción del alumnado se realiza por los mismos estudiantes y de manera totalmente voluntaria (si son mayores de 14 años, o de sus padres o tutores si son menores), estableciendo un vínculo individual basado en una relación contractual (artículo 6.1.b del RGPD) entre el estudiante o sus padres o tutores y el propietario de la plataforma, vínculo en el que no tomaría parte la administración, ni el profesorado tendría ningún tipo de acceso a los resultados del trabajo en línea del estudiantado.

Es decir, sería posible recomendar el uso voluntario de la aplicación por parte de los/las estudiantes, pero no obligarles a utilizarla como parte del proceso educativo.

#### **CASOS PRÁCTICOS: Uso de herramientas de correo electrónico y mensajería instantánea**

LA RESOLUCIÓN de 28 de junio de 2018, de la Subsecretaría de la Conselleria de Educación, Investigación, Cultura y Deporte, por la cual se dictan instrucciones para el cumplimiento de la normativa de protección de datos en los centros educativos públicos de titularidad de la Generalitat, hace referencia clara a la prohibición de utilizar herramientas de mensajería no aprobadas por la Conselleria, tanto para comunicarse con el alumnado como con los familiares:

“A todos los efectos, las comunicaciones entre el profesorado y el alumnado tienen que tener lugar dentro del ámbito de la función educativa y no se tienen que llevar a cabo a través de aplicaciones de mensajería instantánea. Si hubiera que establecer canales específicos de comunicación, tendrán que emplearse las herramientas y los medios establecidos por la conselleria competente en materia de educación y puestos a disposición de alumnado y profesorado o por medio del correo electrónico.”

“Las comunicaciones entre el profesorado y los familiares de alumnos tienen que llevarse a cabo a través de los medios puestos a disposición de los dos por el centro educativo o la conselleria competente en materia de educación.”

Estas obligaciones van en la línea señalada en el apartado "Uso de herramientas de correo electrónico y mensajería instantánea" de la orden 19/2013, de 3 de diciembre, de la Conselleria de Hacienda y Administración Pública, por la cual se establecen las normas sobre el uso seguro de medios tecnológicos en la Administración de la Generalitat:

*Artículo 21. Correo electrónico corporativo.*

*1. Las cuentas creadas en los servidores de la Administración de la Generalitat tienen como objetivo el intercambio de mensajes propios del ejercicio profesional. Queda prohibido su uso con fines comerciales, financieros o personales.*

...

*5. No se permite el uso de cuentas de correo diferentes de los proporcionados por la Administración de la Generalitat dentro de la RCGVA, excepto autorización expresa del órgano con competencias en materia de tecnologías de la información.*

*6. Los usuarios no tienen que enviar mensajes con información sensible tanto en el cuerpo del mensaje como en los archivos adjuntos. Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información sea inteligible o manipulada por terceros (encriptación y firma electrónica).*

...

*8. Para garantizar la identidad del remitente, los correos se firmarán digitalmente.*

Siendo la Red Corporativa de la Generalitat Valenciana la infraestructura común para el interconexión de las sedes de todas las consellerias y organismos, tanto a nivel de los servicios de datos como de voz, con una distribución geográfica que alcanza toda la Comunidad Valenciana, el correo corporativo es el sistema idóneo de comunicación entre el personal para el ejercicio de sus funciones profesionales, gracias al hecho que la información se transmite y almacena utilizando únicamente medios sometidos al control de la administración.

### **CASOS PRÁCTICOS: Uso de cuadernos de notas y seguimiento de la actividad docente**

Existen cuadernos de notas o aplicaciones que permiten el seguimiento de la actividad docente. En algunos casos, la aplicación trabaja exclusivamente en la "nube", con lo cual el proveedor de la misma tendría que ser un encargado del tratamiento (con contrato y garantías suficientes de



seguridad). Hay que tener en cuenta, que la simple realización de una copia de seguridad en la nube implica un tratamiento de datos personales por parte del proveedor.

En otros, la aplicación trabaja solo en local y no da acceso a los datos a los propietarios de esta. Aun así, como ya se ha explicado, el Reglamento General de Protección de Datos también establece que los datos personales tendrán que ser tratados de tal manera que se garantice una seguridad adecuada de estos. El uso de dispositivos personales tales como ordenadores de uso privado, sean portátiles o de sobremesa, *tablets* o teléfonos móviles, puede comprometer la seguridad de los datos personales porque estos dispositivos no están sujetos, a todos los efectos, al cumplimiento de lo que se prevé en el Esquema Nacional de Seguridad. En consecuencia, en estos casos, aunque los datos no se suban a la nube de la empresa, habría que tratarlas en equipos de la Conselleria o del centro que cumplieran con las exigencias del Esquema Nacional de Seguridad.