Guía básica
de protección de datos
para los
centros educativos

apdcat
Autoritat Catalana de Protecció de Dades

Generalitat
de Catalunya

Primera edición: diciembre 2014
Coordinación de la edición y composición: Entitat Autònoma del Diari Oficial i de Publicacions
Depósito legal:

Índice

Presentación

Los centros educativos necesitan tratar información personal para ejercer las funciones que tienen encomendadas. Esta información puede ser de cualquier persona física que se relacione con el centro, pero muy especialmente de sus alumnos. Tratar esta información de forma adecuada se convierte en un objetivo de una importancia primordial, no sólo por el papel de los centros educativos como eje transmisor de los valores que, como la privacidad, están ligados al respeto de los derechos de las personas, tal como recoge la Disposición adicional decimocuarta de la Ley de educación, sino también porque el tratamiento de la información relativa a los menores requiere un especial cuidado. Un tratamiento inadecuado de su información en esta fase de su vida, en la que todavía se están formando, puede acabar afectando al desarrollo de su personalidad en esta etapa y en etapas posteriores de sus vidas.

Con esta guía, dirigida a las personas que forman parte de la estructura organizativa del centro educativo, se quiere ofrecer una herramienta que facilite el cumplimiento de las obligaciones establecidas por la normativa de protección de datos mediante la recopilación de los conceptos, los principios y las obligaciones básicas establecidas por la normativa vigente, con una referencia a la normativa de aplicación y a los informes que ha elaborado la Autoridad Catalana de Protección de Datos en esta materia. Al mismo tiempo también se tratan de manera concreta, en forma de preguntas y respuestas, las principales cuestiones que han planteado los centros educativos públicos y concertados que forman parte del ámbito de actuación de esta Autoridad en relación con el tratamiento de datos personales.

Por otra parte, esta Guía se dirige también a las personas que ocupan cargos o despliegan funciones en las asociaciones de madres y padres de alumnos (AMPA). A estas asociaciones se les aplican los mismos principios y obligaciones que a los centros educativos, aunque con algunas particularidades que se recogen en un apartado específico.

Espero que encontréis en esta Guía una herramienta útil para gestionar la información personal de que disponen los centros educativos y las AMPA, que contribuya al cumplimiento de la normativa de protección de datos y, en definitiva, al respeto por los derechos de las personas.

M. Àngels Barbarà Fondevila
Directora

1 Marco normativo

El tratamiento de datos de carácter personal requiere el cumplimiento de unos principios y unas obligaciones que se regulan en la normativa vigente

1. Normativa europea

- Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas
- Reglamento (UE) nº. 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales, en el marco de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, sobre la privacidad y las comunicaciones electrónicas

2. Normativa estatal

- Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº. 298, de 14.12.1999)
- Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº. 17, de 19.01.2008)

3. Normativa catalana

- Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos (DOGC nº. 5731, de 8.10.2010)
- Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos (DOGC nº. 3835, de 04.03.2003)
- Instrucción 1/2009 de la Agencia Catalana de Protección de Datos, de 10 de febrero de 2009, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia

4. Normativa sectorial

- Ley orgánica 8/1985, de 3 julio, del derecho a la educación
- Ley orgánica 2/2006, de 3 de mayo, de educación
- Ley 12/2009, del 10 de julio, de educación
- Decreto 202/1987, de 19 de mayo, sobre asociaciones de padres de alumnos
- Orden EDU/316/2010, de 27 de mayo, de creación del fichero de datos de carácter personal Proyecto eduCAT 1x1 gestionado por el Departamento de Educación
- Orden ENS/125/2011, de 13 de mayo, de actualización de los ficheros que contienen datos de carácter personal gestionados por el Departamento de Enseñanza
- Orden ENS/59/2014, de 28 de febrero, de regulación de ficheros que contienen datos de carácter personal del Departamento de Enseñanza

5. Recomendaciones de la Autoridad Catalana de Protección de Datos

- Recomendación 1/2013, de la Autoridad Catalana de Protección de Datos, sobre el uso del correo electrónico en el ámbito laboral
- Recomendación 1/2011, de la Autoridad Catalana de Protección de Datos, sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública
- Recomendación 1/2010, de la Agencia Catalana de Protección de Datos, sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña
- Recomendación 1/2008 de la Agencia Catalana de Protección de Datos, sobre la difusión de información que contenga datos de carácter personal a través de Internet

6. Dictámenes e informes de la Autoridad[1]

- CNS 5/2008 cesión de datos a la Consejería de Educación de otra comunidad autónoma, con el fin de informar sobre una oferta educativa en catalán
- CNS 38/2009 tratamiento datos psicopedagógicos en los centros educativos
- CNS 25/2010 cesión de datos de una escuela municipal de danza a un ayuntamiento
- CNS 31/2010 comunicación a un ciudadano de los listados de preinscripciones escolares
- CNS 44/2010 videovigilancia en los centros educativos
- CNS 27/2011 protocolo en los centros educativos para detectar jóvenes que pueden formar parte de grupos violentos
- CNS 28/2011 utilización del número de DNI como *login* para acceder a una intranet
- CNS 29/2011 publicación de las evaluaciones de los docentes que hacen los alumnos de la Universidad
- CNS 41/2011 difusión de datos de alumnos en la intranet de una universidad
- CNS 40/2012 cesión a un ayuntamiento de datos de matriculación en centros escolares del municipio para el otorgamiento de ayudas individuales
- CNS 19/2013 publicación de resolución de concesión de ayudas escolares
- CNS 23/2013 acceso de un concejal a expedientes de concesiones de ayudas escolares
- CNS 37/2013 responsabilidad de la gestión del blog de un jardín de infancia municipal

1. Se puede consultar éstos y otros dictámenes e informes emitidos con posterioridad a la edición de esta Guía, en http://www.apd.cat

- CNS 42/2013 competencia de la APDCAT sobre los ficheros de una fundación que gestiona un centro concertado y plazo de conservación de expedientes escolares de alumnos
- CNS 14/2014 comunicación de datos del Padrón Municipal de Habitantes a un centro escolar público del municipio para recordar a las familias el periodo de preinscripción escolar
- CNS 16/2014 comunicación a los servicios sociales de datos de menores en situación de riesgo o desamparo
- PET 5/2009 naturaleza jurídica de los ficheros del AMPA
- PET 8/2011 competencia sobre los ficheros de una guardería privada que recibe subvenciones públicas
- PET 10/2011 competencia de la APDCAT sobre ficheros de escuelas concertadas
- PET 6/2012 competencia de la APDCAT sobre los ficheros de los consejos deportivos

2 Tratamiento de datos en los centros educativos

Los centros educativos necesitan tratar datos personales para ejercer sus funciones

El derecho a la protección de datos de carácter personal es un **derecho fundamental** reconocido jurisprudencialmente a partir de lo que establece el artículo 18.4 CE, recogido en el EAC y desarrollado por la LOPD. Este derecho quiere garantizar que las personas físicas tengan conocimiento sobre quién dispone de sus datos y con qué finalidad, para poder tener capacidad de decisión sobre el tratamiento de esta información.

Tratamiento de datos personales

Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan recoger, grabar, conservar, elaborar, modificar, bloquear y cancelar los datos, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Tratar información personal quiere decir acceder a esta información (ya sea porque la misma persona interesada, o sus representantes legales, la facilita al centro educativo o porque el centro la recibe de terceras personas), así como almacenarla, modificarla, utilizarla, eliminarla o comunicarla a cualquier tercero ajeno a la persona jurídica de que forma parte el centro.

En este sentido, para cumplir con las obligaciones establecidas por la normativa de protección de datos, hay que identificar los datos que se tratarán y que se tienen que proteger. También conocer los conceptos básicos, los principios fundamentales y las obligaciones establecidas para garantizar la protección de la información de las personas interesadas o afectadas.

El centro educativo puede tener un papel fundamental en la garantía de este derecho, no sólo como responsable del tratamiento adecuado de la información de las personas que se relacionan con ella, sino también como elemento esencial en su difusión, dado que puede permitir que la sociedad, ya desde el momento de su

formación en los centros educativos, lo conozca y lo utilice. El centro educativo se tiene que convertir en un elemento clave en la difusión de este derecho fundamental.

Normativa aplicable: art. 18.4 CE; 31 EAC; 1, 3.c), d) y e) LOPD; 5.1.a), q) y t) RLOPD; SSTC 290/2000 y 292/2000.

2.1 Datos de carácter personal

Para ejercer sus funciones, los centros educativos tratan datos de diferentes colectivos y de diferentes tipologías.

Estas funciones pueden ser, a modo de ejemplo:

- Admisión de alumnos: publicidad y contacto con personas interesadas en incorporarse al centro, proceso de preinscripción, matriculación
- Gestión académica
- Servicios ofrecidos por el centro educativo a los alumnos y que completan la finalidad educativa: comedor, transporte escolar, actividades extraescolares, etc.
- Gestión del personal docente, administrativo y de servicios
- Gestión de proveedores
- Servicios a exalumnos

Los colectivos sobre los cuales tratan datos son los alumnos, los padres y madres de alumnos, los profesores, los tutores, los otros trabajadores de los centros, los proveedores, los asistentes a actividades, los exalumnos o las otras personas con las cuales se relacionan.

En el caso de los datos de los alumnos, el tratamiento de datos en los centros educativos se produce por primera vez cuando los padres o tutor solicitan una plaza en el proceso de preinscripción, y se mantiene hasta que el alumno finaliza los estudios en aquel centro. Eso comporta el tratamiento de mucha información, ya sea facilitada por la familia, por los profesionales que trabajan en el centro (profesores, tutores, psicólogos, etc.) o por los mismos alumnos con motivo del desarrollo de la actividad del centro (pruebas, actitud, aptitudes, preferencias, enfermedades, expediente académico, etc.).

Los centros educativos pueden tener que tratar diferentes categorías de datos:

- Datos identificativos
- Datos de características personales
- Datos de circunstancias sociales
- Datos académicos y profesionales
- Datos económico-financieros
- Datos de ocupación laboral
- Datos especialmente protegidos: datos de salud, ideología, afiliación sindical, religión, creencias, vida sexual, origen racial, comisión de infracciones penales o administrativas

La información referida a personas físicas puede ser de diversos tipos (numérica, alfabética, gráfica, fotográfica, acústica) y puede referirse a un rasgo físico de la persona, a su capacidad intelectual, a sus gustos y preferencias, a su actividad, a su situación económica o social, a sus estudios, a su profesión, a su salud, etc.

La información puede permitir identificar directamente a una persona (cuando disponemos del nombre y apellidos, de una fotografía, del DNI, etc.), o bien puede identificarla indirectamente (cuando disponemos de una información que no está vinculada directamente a una persona concreta, pero la asociamos con otros datos que sí que nos permiten identificarla sin esfuerzos desproporcionados).

La mayor parte de los datos tratados en los centros educativos son de menores de edad. Eso hace que, por la vulnerabilidad de este colectivo y las consecuencias que se pueden derivar de un tratamiento inadecuado, los centros educativos tengan que extremar, todavía más que en otros ámbitos, la diligencia en el tratamiento de esta información.

La captación de imágenes de personas físicas o su voz mediante cámaras u otros dispositivos electrónicos constituye también un tratamiento específico de datos personales, que puede tener sus propias especificidades y al cual se dedica el apartado 9 de esta Guía.

La LOPD protege toda esta información, salvo los datos que no se pueden relacionar con una persona concreta sin esfuerzos desproporcionados.

Dato personal

Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Persona identificable

Cualquier persona cuya identidad puede determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.

Por otra parte, las asociaciones de madres y padres de alumnos también tratan información personal para ejercer sus funciones. En este caso, tratan datos tanto de los padres y madres como de los alumnos o de terceros con quien se relacionan. Por eso, el apartado 10 de esta Guía se dedica de manera específica a los tratamientos de datos que hacen estas asociaciones.

Normativa aplicable: art. 3.a) LOPD; DA 14ª LE; 15.3 LTAIBG, 2.2, 2.3, 5.1.e), f) y o) RLOPD.

2.2 Datos especialmente protegidos

Para ejercer sus funciones, los centros educativos pueden tener que tratar información que la normativa de protección de datos califica como datos especialmente protegidos.

De acuerdo con la normativa de protección de datos, tienen esta consideración los relativos a:

- La ideología
- La afiliación sindical
- La religión y las creencias
- El origen racial
- La salud
- La vida sexual
- La comisión de infracciones penales y administrativas

> **Dato personal relacionado con la salud**
>
> Informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

El tratamiento de este tipo de información, directamente vinculada con otros derechos fundamentales como la libertad ideológica o religiosa o la prohibición de discriminación por razón de raza, sexo, religión o cualquier otra circunstancia personal o social, requiere una rigurosidad especial en el cumplimiento de los principios de la protección de datos y está sometido a unas condiciones especiales, tanto con res-

pecto a la forma como se tiene que obtener el consentimiento, como a las medidas de seguridad aplicables. En el caso de las infracciones penales y administrativas, además, sólo las administraciones públicas competentes pueden crear ficheros para recopilar estos datos, de acuerdo con las normas que las regulan.

En el ámbito educativo resulta especialmente relevante el tratamiento de datos relativos a la salud de los alumnos. Así, por ejemplo, datos referidos a necesidades educativas especiales, como alguna minusvalía, u otros como alergias e intolerancias, así como los datos contenidos en los informes psicopedagógicos de los alumnos, etc., tienen la consideración de datos relativos a la salud de los alumnos. Los centros educativos y en concreto las personas que tienen que cuidar de los menores, pueden tener que conocer si sufren determinadas enfermedades o alergias, pero hay que adoptar las medidas para que esta información se trate con las máximas garantías posibles.

Por eso, y de acuerdo con los padres de los alumnos afectados, hay que establecer los protocolos necesarios para tratar adecuadamente esta información, tanto durante el funcionamiento normal del centro (estancia en las aulas, horario de esparcimiento, educación física, comedor, enfermería, evaluación psicopedagógica, etc.) como en situaciones extraordinarias (sustituciones de maestros o tutores, celebraciones de aniversarios, salidas, colonias, etc.).

◊ **¿Los datos sobre sanciones disciplinarias a alumnos se consideran datos especialmente protegidos?**

No. El artículo 7.5 de la LOPD se refiere sólo a sanciones penales o administrativas. No obstante, y vista la incidencia que la divulgación de información asociada a las sanciones disciplinarias puede tener en el desarrollo del menor, se recomienda mantener una diligencia especial en el tratamiento de esta información.

◊ **¿El seguimiento de una dieta específica se puede considerar un dato relativo a la salud o a las creencias de una persona?**

Sí, si el seguimiento de la dieta puede asociarse a una enfermedad específica. En otros casos, el seguimiento de determinadas dietas puede asociarse a la

religión de una persona. En ambos casos, nos encontraríamos ante datos que deben ser especialmente protegidos.

◊ **¿La elección de la asignatura de religión por parte de un alumno se puede considerar como un dato personal relativo a la religión o a las creencias?**

No. Este dato, aisladamente considerado, no tiene la consideración de dato especialmente protegido.

Normativa aplicable: art. 7 LOPD; 5.1.g) RLOPD; CNS 38/2009.

2.3 Los sujetos implicados: quién es quién

En el tratamiento de los datos personales hay diversos sujetos implicados:

Afectado o interesado

Persona física titular de los datos que sean objeto del tratamiento.

Los datos de carácter personal que los centros educativos tratan para ejercer sus funciones no pertenecen al centro, sino a los alumnos, a sus familiares, a su personal o a otras personas físicas con las cuales se relacionan. Éstos son los auténticos titulares de su información personal.

Responsable del fichero o del tratamiento

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no trate los datos materialmente. También pueden ser responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Establecer quién es el órgano responsable del fichero o del tratamiento, por lo tanto el órgano que tiene que decidir sobre los diferentes aspectos relativos al tratamiento de la información, es una decisión organizativa que se tiene que adecuar a las necesidades, las normas y los criterios por los cuales se rige cada organización.

En el caso de los centros educativos públicos, pueden depender de un departamento de la Administración de la Generalitat, pero al mismo tiempo tienen atribuida una cierta autonomía en su gestión. Por eso, es posible que el departamento correspondiente establezca que el responsable del fichero sea un órgano de la estructura central del departamento, o bien un órgano de cada centro educativo.

Actualmente el responsable de los ficheros de los centros educativos que dependen del Departamento de Enseñanza está establecido en la Orden EDU/316/2010, de 27 de mayo, la Orden ENS/125/2011, de 13 de mayo y la Orden ENS/59/2014.

En el caso de los centros concertados, el responsable de sus ficheros es el órgano que cada centro determine.

En determinados casos, para cumplir sus funciones, los centros educativos necesitan contar con la colaboración de otras personas o entidades que no forman parte de la organización. En este caso, si esta colaboración requiere tratar datos que son responsabilidad del centro educativo, nos encontraremos delante de la figura del encargado del tratamiento.

Encargado del tratamiento

Persona física o jurídica, pública o privada, u órgano administrativo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

También pueden ser encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Las cuestiones relativas al encargado del tratamiento se tratan de forma específica en el apartado 5.3 de esta Guía.

Tercero

Persona física o jurídica, pública o privada, u órgano administrativo diferente del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

También pueden ser terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

◊ **¿Quién es el responsable del fichero de una escuela municipal de danza gestionada por una empresa privada a través de una concesión?**

Depende de la forma cómo lo hayan configurado las entidades implicadas. En principio la empresa que gestiona el servicio puede ser la responsable del fichero. Ahora bien, como se trata de un servicio municipal, se tendría que haber configurado como un fichero municipal. En este caso sería un fichero de titularidad pública, y la escuela de danza actuaría como un encargado del tratamiento, a través de la firma de un acuerdo de encargo en los términos que establece el artículo 12 LOPD.

◊ **¿Una empresa que presta servicios de evaluación psicológica por encargo de un centro educativo es la responsable del fichero donde se introducen los datos de los alumnos evaluados, o sólo es la encargada del tratamiento?**

Si se establece el acuerdo o contrato de encargo del tratamiento previsto en el artículo 12, tiene la consideración de encargada del tratamiento. De lo contrario, es responsable.

◊ **¿Quién es el responsable del fichero o de los ficheros que contienen los datos personales que se integran en la plataforma de gestión académica contratada por el centro educativo?**

El centro educativo es el responsable de estos ficheros y la empresa con la que ha contratado la plataforma será la encargada del tratamiento si se establece el acuerdo de encargo en los términos del artículo 12 LOPD.

Normativa aplicable: art. 3.d), e) y g) LOPD; 5.1.a), i), q) y r) RLOPD; la Orden EDU/316/2010, de 27 de mayo, la Orden ENS/125/2011, de 13 de mayo y la Orden ENS/59/2014; CNS 25/2010.

3 Legitimidad del tratamiento

Los centros educativos pueden tratar los datos personales adecuados para ejercer sus funciones

3.1 El principio de consentimiento

3.1.1 El consentimiento

El consentimiento es la pieza angular en la protección de datos. Constituye el principio sobre el cual se articula el poder de disposición y control de cualquier persona sobre sus datos. Así, cuando el centro educativo tiene que tratar datos de carácter personal para ejercer sus funciones, tiene que contar con el consentimiento de la persona afectada o, si no, con una ley que lo habilite.

> **Consentimiento de la persona afectada**
>
> Cualquier manifestación de la voluntad, libre, inequívoca, específica e informada, mediante la que la persona interesada consienta el tratamiento de datos personales que le conciernen.

De acuerdo con la normativa de protección de datos, el consentimiento tiene que ser:

- **Inequívoco:** la solicitud y el otorgamiento del consentimiento se tienen que producir de forma clara.
- **Libre:** la persona tiene que tener la posibilidad de rechazar libremente que se traten sus datos.
- **Específico:** el consentimiento se refiere a tratamientos concretos y para una finalidad determinada, explícita y legítima del responsable del tratamiento, sin que se puedan hacer habilitaciones genéricas.
- **Informado:** hay que informar a las personas afectadas de acuerdo con lo que establece el artículo 5 de la LOPD para que, antes de iniciar el tratamiento, puedan conocer su existencia y sus finalidades.

La solicitud del consentimiento se tiene que referir a un tratamiento o una serie de tratamientos concretos, con delimitación de la finalidad para la cual se pide, y del resto de condiciones que concurren en el tratamiento.

Asimismo, la normativa de protección de datos prevé la necesidad de solicitar el consentimiento de los interesados cuando se hagan o se prevean cesiones o comunicaciones de datos a terceros, a menos que una ley las autorice.

◊ **Un centro educativo obtiene el consentimiento para utilizar la imagen de unos alumnos con finalidades publicitarias del centro. ¿Puede cederlas, sin consentimiento, a una productora de TV para hacer un documental?**

No. La solicitud del consentimiento siempre se tiene que referir a una finalidad o finalidades determinadas, explícitas y legítimas. Puede referirse además de un tratamiento a la vez, pero tienen que estar perfectamente determinados. Cuando se pida en el mismo momento para diferentes finalidades, el consentimiento tiene que poder ser independiente para cada una. Así, los padres tienen que poder consentir que el centro difunda la imagen con finalidades publicitarias y, al mismo tiempo, no consentir otros usos de la imagen del hijo que vayan más allá de este tratamiento.

◊ **¿Cuando sea necesario el consentimiento para tratar los datos, el centro educativo tiene que contar siempre con la autorización de los dos padres?**

El tratamiento de los datos de un menor de 14 años, lo puede autorizar cualquiera de los padres, siempre que tenga la patria potestad. Cuando el hijo tenga más de 14 años su consentimiento es suficiente para tratar sus datos, salvo los casos en que una ley exija la asistencia de los padres o tutor.

◊ **¿Hace falta el consentimiento de los padres para tratar los datos de salud del alumno, concretamente los datos psicopedagógicos?**

No hace falta el consentimiento si el tratamiento es efectivamente necesario para ejercer las funciones docente y orientadora del centro.

3.1.2 La obtención del consentimiento

El consentimiento se puede obtener de forma **expresa** (por ejemplo, en el mismo formulario de recogida de datos) **o tácita**, a menos que se trate de datos especialmente protegidos. En este último caso, el consentimiento tiene que ser expreso.

Corresponde al responsable del fichero probar que ha obtenido el consentimiento del interesado para un tratamiento específico.

Los datos de menores

Los centros educativos normalmente tratan datos de menores de edad. Con respecto al consentimiento para tratarlos, hay que tener en cuenta lo siguiente:

- Si son **mayores de 14 años**, es suficiente con su consentimiento, salvo los casos en que la ley exija la asistencia de las personas titulares de la patria potestad.
- Si son **menores de 14 años**, siempre hace falta el consentimiento de los padres o tutor.

A través de un menor no se pueden recoger datos que permitan obtener información sobre el resto de miembros del grupo familiar o sobre sus características (actividad profesional de los progenitores, información económica, etc.), sin consentimiento de las otras personas afectadas, a menos que se trate de los datos referentes a la identidad y la dirección de los progenitores para poder obtener su consentimiento.

La protección de los menores se concreta, también, en la exigencia que la información que se les proporciona sea en un lenguaje que les resulte fácilmente comprensible.

◊ ¿Se pueden recoger datos personales directamente del menor, sin autorización de sus padres o tutor?

No, en el caso de los menores de 14 años. En este caso hay que contar con el consentimiento del padre, madre o tutor.

Sí, en el caso que sean mayores de 14 años. Los datos se pueden recoger directamente con el consentimiento del menor, salvo los casos en que la ley exige para su prestación la asistencia de los titulares de la patria potestad o tutela.

◊ ¿Se pueden pedir al menor datos de sus padres?

A través de un menor no se pueden recoger datos que permitan obtener información sobre el resto de miembros del grupo familiar o sus características sin consentimiento de las otras personas afectadas. Sólo se le puede pedir el nombre y apellidos y la dirección de los padres o tutor, para obtener su consentimiento.

◊ ¿Un centro educativo puede recoger el dato relativo a las direcciones de los correos electrónicos de los padres a través de los alumnos menores de edad, con el fin de ponerse en contacto con ellos?

Como norma general, hay que contar con el consentimiento de los padres para recoger el dato relativo a su correo electrónico. Excepcionalmente, puede facilitarlo directamente el menor, en aquellos casos en que sea necesario completar la capacidad del menor de edad a través de sus progenitores, a fin de que éstos puedan consentir el tratamiento de los datos del menor.

◊ ¿Puede el personal docente de un centro educativo exigir a un menor de 14 años la clave de acceso a su cuenta de una red social y consultar su contenido sin el consentimiento de sus padres o tutor?

No, el acceso y la consulta del contenido de la cuenta, de una red social de un alumno menor de 14 años en principio no formaría parte de la acción educativa u orientadora del centro, a menos que se trate de una cuenta facilitada por el mismo centro con finalidades académicas. Cuando la gravedad de las circunstancias lo requiera, hay que contar con el consentimiento de los padres o tutor.

Los datos especialmente protegidos

Es muy probable que los centros educativos, para ejercer sus funciones ya desde el inicio del ciclo escolar tengan que tratar datos que tienen la consideración de datos especialmente protegidos. Son datos de salud de los alumnos, discapacidades, exámenes psicopedagógicos, enfermedades crónicas, intolerancias alimenticias, datos de religión y creencias, origen racial de los alumnos, así como infracciones penales y administrativas o datos de la afiliación sindical de los maestros y trabajadores.

Estos datos especialmente protegidos se pueden tener que tratar, tanto en el momento de la preinscripción y la matriculación como después, durante el ciclo académico.

Así, en el momento de la preinscripción, con la finalidad de determinar la puntuación que corresponda para acceder a un determinado centro o de llevar a cabo las adaptaciones apropiadas, se pueden tener que tratar datos relativos a una discapacidad, a una enfermedad crónica que afecte al sistema endocrino o metabólico del alumno y que exija un control alimentario o la existencia de necesidades educativas especiales derivadas de la pertenencia a una minoría étnica o inmigrante con déficit social o cultural.

Por otra parte, durante la actividad docente se recogen datos sobre enfermedades o discapacidades de los alumnos a través de la información que facilitan los padres y los alumnos o a través del servicio médico o de enfermería del centro, así como informaciones psicológicas derivadas del seguimiento del alumno, etc.

La LOE habilita los centros educativos para tratar datos especialmente protegidos de sus alumnos, que pueden incluir datos referentes al origen y al ambiente familiar y social, a características o condiciones personales y al desarrollo y a los resultados de su escolarización, así como otras circunstancias cuyo conocimiento sea necesario para la educación y la orientación de los alumnos.

Más allá de eso, en los casos en que haga falta el consentimiento de las personas afectadas, hay exigencias especiales con respecto a la forma de recoger el consentimiento:

a) **Datos sobre ideología, afiliación sindical, religión y creencias** de una persona física: sólo pueden tratarse con el consentimiento expreso y por escrito del titular de los datos, y advirtiéndole respecto de su derecho a no facilitar estos datos.

b) **Datos sobre origen racial, salud y vida sexual** de una persona física: sólo se pueden tratar cuando, por razones de interés general, así lo disponga una ley o la persona afectada consienta expresamente.

La legislación otorga también una protección especial a los datos relativos a infracciones administrativas y penales, al establecer que sólo se pueden incluir en los ficheros de las administraciones públicas competentes en los supuestos previstos en las normas reguladoras respectivas.

Conviene tener en cuenta sin embargo, que los datos especialmente protegidos se pueden tratar sin consentimiento cuando sea necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o de tratamientos médicos por parte de profesionales sanitarios u otras personas sujetas al secreto profesional. También para salvaguardar el interés vital de la persona afectada o de otra persona, en caso de que esté físicamente o jurídicamente incapacitada para dar el consentimiento.

◊ **¿Hace falta el consentimiento para tratar datos psicológicos del alumno mediante la realización de pruebas psicotécnicas al alumno?**

No. La LOE excluye la necesidad del consentimiento para tratar los datos necesarios para ejercer las funciones docentes y orientadores.

◊ **¿Hace falta el consentimiento para tratar datos de los alumnos con necesidades educativas especiales?**

No. La LOE habilita el uso de los datos de los alumnos y familiares para darles la atención que necesitan, siempre que se utilicen únicamente y exclusivamente con una finalidad docente y orientadora.

◊ **¿Para comunicar datos de un alumno a un centro hospitalario si necesita atención médica urgente, hace falta su consentimiento o el de sus padres?**

No. Excepcionalmente, los datos especialmente protegidos se pueden tratar, sin consentimiento, cuando sea necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o de tratamientos médicos, la gestión de servicios sanitarios, por parte de profesionales sanitarios u otras personas sujetas al secreto profesional, o para salvaguardar el interés vital de la persona afectada o de otra persona, en caso de que esté física o jurídicamente incapacitada para dar su consentimiento.

El consentimiento tácito

Cuando el consentimiento tácito sea admisible, se puede obtener a través del mecanismo siguiente:

a) El responsable del tratamiento se puede dirigir a las personas afectadas, informarles en los términos del art. 5 LOPD y otorgarles un plazo de 30 días hábiles por manifestar su negativa al tratamiento. Conviene que el medio utilizado permita dejar constancia que el afectado lo ha recibido.

b) Se tiene que ofrecer a la persona interesada un medio sencillo y gratuito para manifestar su negativa al tratamiento de sus datos en el plazo mencionado. Conviene que este medio permita dejar constancia de su recepción.

c) Si la persona interesada manifiesta su negativa, el responsable del fichero no puede volver a pedirle el consentimiento respecto del mismo tratamiento y las mismas finalidades, en el plazo de un año a contar desde la fecha de la solicitud anterior.

d) Si la persona interesada no se ha pronunciado al acabar el plazo, se entiende que consiente el tratamiento de los datos.

El consentimiento tácito no es admisible respecto de los datos calificados como especialmente protegidos.

◊ **¿Cómo puede probar el centro que ha obtenido el consentimiento del alumno para un tratamiento concreto?**

A través de cualquier medio admisible en derecho.

Por ejemplo, mediante los mismos formularios en papel que el centro utiliza en la recogida de los datos. Si el consentimiento se ha solicitado mediante el procedimiento del artículo 14 del RLOPD, se puede probar, entre otros medios, a través del acuse de recepción de la comunicación que el centro ha enviado por correo postal certificado.

◊ **¿Hace falta el consentimiento para crear direcciones de correo electrónico a menores de edad en el marco de un programa que promueve el uso de las nuevas tecnologías?**

Sí, hace falta el consentimiento del titular de los datos, o de sus padres o tutor si es menor de 14 años, para tratar los datos de los alumnos asociados a la creación de una cuenta de correo electrónico, si esta cuenta se puede utilizar para finalidades que vayan más allá de la actividad académica.

Ahora bien, si se trata de una cuenta de correo otorgada por el mismo centro en el marco de su actividad docente y con un uso limitado a esta finalidad, el consentimiento no es necesario.

3.1.3 La revocación del consentimiento

La persona afectada puede **revocar** el consentimiento otorgado en cualquier momento, sin efectos retroactivos, siempre que haya una causa justificada:

- El responsable del fichero tiene que establecer un medio sencillo a través del cual la persona interesada pueda revocar el consentimiento. El responsable del fichero dispone de un plazo de 10 días hábiles, desde que recibe la solicitud, para cesar en el tratamiento y, si procede, para cancelar los datos.
- La persona interesada puede solicitar al responsable del tratamiento la confirmación del cese. Esta solicitud se tiene que responder expresamente.

- Si el responsable del tratamiento, previamente a la revocación del consentimiento, ha cedido los datos a un tercero, tiene que comunicarle la revocación del consentimiento dentro del mismo plazo de 10 días, para que también deje de tratarlos y, si procede, los cancele.

La revocación del consentimiento impide que se continúen tratando los datos personales, pero no puede evitar los efectos ya producidos por los tratamientos anteriores al momento de la revocación.

3.1.4 Supuestos en que no es necesario obtener el consentimiento

Hay una serie de supuestos regulados en la LOPD en los cuales no es necesario el consentimiento de la persona afectada para tratar sus datos personales. Concretamente no hace falta el consentimiento cuando:

- Así lo establece una **norma con rango de ley**.
- Se recogen para ejercer **funciones propias de las administraciones públicas** en el ámbito de sus competencias.
- Se refieren a las partes de un contrato o precontrato de una **relación laboral**, **negocial o administrativa** y son necesarios para mantenerla o cumplirla.
- El tratamiento de los datos tiene como finalidad proteger un **interés vital** del interesado.
- Los datos figuren en **fuentes accesibles al público** y haya que tratarlos para satisfacer un interés legítimo perseguido por el responsable del fichero. Son fuentes accesibles al público: el censo promocional, las guías de servicios de comunicaciones electrónicas, las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos del nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo, los diarios y boletines oficiales y los medios de comunicación social.

- El tratamiento tiene por objeto la satisfacción de un **interés legítimo** del responsable del tratamiento o del cesionario amparado por estas normas, siempre que no prevalezcan el interés o los derechos y las libertades fundamentales de los interesados.

Los datos sobre origen racial, salud y vida sexual sólo se pueden tratar sin consentimiento expreso de las personas afectadas cuando, por razones de interés general, así lo dispone una ley.

En el caso de los centros educativos, normalmente los datos de los alumnos se tratan con el consentimiento de las personas afectadas o porque la ley, como es el caso de la LOE, habilita el tratamiento.

Así, de acuerdo con la LOE, la incorporación de un alumno a un centro docente supone el consentimiento para tratar sus datos estrictamente necesarios para la función docente y orientadora y, si procede, para la cesión de datos procedentes del centro donde haya sido escolarizado anteriormente.

Los centros docentes, sean de titularidad pública o privada, pueden recoger, sin consentimiento, los datos personales de su alumnado necesarios para ejercer su función educativa. Estos datos pueden hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y a los resultados de su escolarización, así como otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.

Los padres o el tutor y los mismos alumnos tienen que colaborar en la obtención de la información.

Para otros casos en que hay que tratar los datos con finalidades diferentes a la función docente y orientadora, como la publicación de fotografías en el web del centro o la entrega de datos a casas de colonias, museos u otros establecimientos que se visiten, se necesita el consentimiento del titular de los datos, o de su representante en el caso de los menores de 14 años.

Con respecto a los datos relativos a sus trabajadores, los centros educativos pueden tratar los de su personal sin necesidad de su consentimiento, por ejemplo, en aplicación de las excepciones al consentimiento previstas en la LOPD, cuando los datos sean necesarios para mantener o cumplir la relación laboral o administrativa que mantienen con el centro.

◊ **¿El alumno/los padres, se pueden negar a dar el consentimiento para que el centro educativo trate sus datos?**

No. Los centros educativos están habilitados legalmente para tratar los datos que sean necesarios para ejercer su función docente y orientadora.

◊ **¿El centro educativo necesita el consentimiento de sus trabajadores para tratar sus datos?**

No. El centro está legitimado para recoger y tratar los datos de sus trabajadores necesarios y adecuados para cumplir con la relación laboral que se establece con estos trabajadores.

Normativa aplicable: art. 3. j), 6 y 7 LOPD; 7.1.f) Directiva 95/46/CE; DA 23ª LOE; 5.1.d), 7 y 12 y ss. RLOPD; STJUE 24.11.2011.

3.2 El principio de calidad de los datos

Es el segundo de los principios primordiales con respecto al derecho fundamental a la protección de datos. En realidad se trata de un principio que se desgrana en una serie de principios regulados en la LOPD y en el RLOPD. El objetivo es que se utilicen sólo los datos imprescindibles para alcanzar una finalidad determinada, que se traten sólo durante el tiempo estrictamente necesario, y que sean exactos y actualizados.

En este sentido, la misma LOE establece que la información que recojan los centros docentes en ejercicio de su función educativa tiene que ser la estrictamente necesaria para la función docente y orientadora, y no se puede tratar con finalidades diferentes de la educativa sin consentimiento expreso.

Hay que revisar con cuidado los datos que se pretende recoger con cada formulario para que se recojan sólo los que, de acuerdo con el principio de calidad de los datos, sean necesarios para alcanzar la finalidad perseguida.

3.2.1 El principio de proporcionalidad

Sólo se pueden tratar los datos que sean **adecuados**, **pertinentes** y **no excesivos** en relación con la finalidad del tratamiento.

◊ **¿El centro puede recoger cualquier tipo de información sobre los alumnos?**

De acuerdo con el principio de calidad de los datos, el centro sólo puede recoger y tratar los datos que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades relacionadas con su actividad.

El principio de calidad no limita el número ni el tipo de datos que pueden recogerse, sino que sólo exige evaluar su proporcionalidad a la vista de la finalidad educativa y de orientación para la cual se recogen.

◊ **¿Cuáles son los datos necesarios, adecuados y pertinentes que hay que tratar en un procedimiento de admisión de alumnos?**

Aparte de los datos identificativos, especialmente el domicilio, hace falta tratar sólo los datos necesarios para determinar si se cumplen los requisitos para adjudicar la plaza y hacer la baremación de las solicitudes según la normativa.

Podría ser desproporcionado, por ejemplo, recoger información sobre ideología, creencias o relaciones personales que no esté expresamente prevista en la normativa reguladora del proceso.

◊ **¿Se pueden utilizar datos biométricos (p. ej. huellas dactilares) de los alumnos para hacer el control horario?**

No. El centro puede utilizar otros mecanismos menos invasivos de la esfera personal del menor, como el control por los profesores.

◊ **¿Y en el caso de los trabajadores del centro? ¿Se pueden utilizar datos biométricos para hacer el control horario?**

Sí. En este caso, la jurisprudencia ha venido admitiendo la utilización de sistemas biométricos para hacer el control horario, si bien hay que respetar las obligaciones establecidas en la normativa de protección de datos (deber de información, creación y notificación del fichero, medidas de seguridad, etc.).

3.2.2 El principio de finalidad

Los datos personales recogidos sólo pueden utilizarse para la **finalidad determinada**, **explícita y legítima** que motivó su recogida. Cualquier uso de los datos para una finalidad incompatible con aquélla para la cual se recogieron es contrario a este principio.

Esta finalidad determinada se tiene que describir en la cláusula informativa correspondiente y en la disposición de carácter general o el acuerdo de creación del fichero que contiene los datos o, en el caso de ficheros de titularidad privada, en el formulario de notificación del fichero.

No se considera incompatible el uso posterior de los datos para finalidades históricas, estadísticas o científicas.

◊ **¿Un centro educativo puede utilizar el dato del correo electrónico de los padres para enviar información sobre actividades extraescolares organizadas por el centro o por el AMPA?**

Sí, porque se trata de una finalidad compatible con la del fichero de alumnos.

◊ **¿Se puede utilizar el fichero de personal docente para enviar información sobre convocatorias de formación del profesorado?**

Sí. Si se trata de un fichero creado para la gestión de personal, eso incluye también la formación del personal.

◊ **¿Los maestros en prácticas, pueden utilizar datos personales que obtengan en su tarea de prácticas para hacer trabajos para la Universidad?**

No. Necesitan el consentimiento de los titulares de los datos. Si no lo tienen, los pueden utilizar si están disociados y no permiten la identificación de las personas titulares de los datos.

◊ **¿Se pueden utilizar los datos de los alumnos para hacer un estudio sobre el fracaso escolar?**

Sí, si bien hay que elaborarlo con datos anonimizados.

◊ **¿Y para que otro centro educativo que ofrece estudios de formación profesional haga una campaña publicitaria entre estos alumnos?**

No, dado que se trataría de una finalidad incompatible, a menos que se obtenga su consentimiento.

3.2.3 Principio de exactitud

Los datos personales que se tratan tienen que ser **exactos y actualizados**, de manera que reflejen la situación real de las personas afectadas. Los datos recogidos directamente del afectado o el interesado en principio se consideran exactos.

Cuando los datos sean inexactos se tienen que rectificar, a petición de la persona afectada en ejercicio de su **derecho de rectificación** o bien de oficio, en el mismo momento en que la entidad responsable del tratamiento tenga conocimiento de la inexactitud.

- Si los datos son o se convierten en inexactos, del todo o en parte, o incompletos, se tienen que **rectificar de oficio**.
- Si los datos ya no son necesarios o pertinentes de acuerdo con la finalidad para la cual se recogieron, se tienen que **cancelar**.

La falta de actualización de los datos personales puede afectar a la misma gestión académica o, incluso puede comportar la revelación indebida de datos a terceras personas (p. ej. si la dirección no está actualizada o no se han comunicado al centro educativo cambios que afectan al régimen legal de patria potestad sobre los menores).

◊ ¿Hace falta que los padres comuniquen al centro educativo los cambios que afectan al ejercicio de la patria potestad de menores escolarizados?

Sí. No disponer de esta información actualizada puede afectar a la gestión adecuada del centro y de la información personal del alumno.

3.2.4 La conservación

Los datos se tienen que cancelar cuando dejen de ser necesarios o pertinentes para la finalidad para la qual se recogieron. Una vez cumplido el periodo de tratamiento, sólo se pueden conservar si se disocian o cuando el tratamiento de los datos atienda a valores históricos, estadísticos o científicos de acuerdo con la legislación específica, solicitando autorización a la Autoridad Catalana de Protección de Datos.

Asimismo, los datos se pueden conservar bloqueados, si procede, durante el tiempo en que se pueda exigir algún tipo de responsabilidad derivada de una relación u obligación jurídica, de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

No obstante, si los datos se han obtenido por medios fraudulentos, desleales o ilícitos, se tienen que destruir directamente.

Sobre esta cuestión, consultar también el apartado 6 *"obligaciones una vez ha finalizado el tratamiento de los datos".*

3.2.5 El principio de lealtad

Cualquier centro educativo que trate datos personales lo tiene que hacer de manera leal y lícita y sin utilizar medios fraudulentos al recogerlos. La vulneración de este principio está tipificada como una infracción muy grave.

Normativa aplicable: art. 4, 44.4.a) y c) LOPD; DA 23ª LOE; art. 8 RLOPD.

4 Obligaciones previas al tratamiento de los datos

Antes de iniciar la recogida de los datos, hace falta crear el fichero, notificarlo a la Autoridad Catalana de Protección de Datos e informar a las personas afectadas

Antes de emprender cualquier actuación que implique el tratamiento de datos de carácter personal, el responsable del tratamiento tiene que hacer una serie de actuaciones:

1. Hacer un **análisis** del "ciclo de vida" o recorrido de los datos a lo largo de su tratamiento, con el fin de identificar:
   - Qué datos personales se tienen que recoger y para qué finalidad.
   - Cómo se recogerán (formularios en papel, electrónicamente, telefónicamente...).
   - Qué ficheros hay que crear y, si procede, qué ficheros hace falta modificar o suprimir.
   - Quién los tratará (áreas, departamentos, personas usuarias ...).
   - Cómo circularán dentro de la entidad (en soporte papel, telemáticamente...).
   - A quién se cederán o qué transferencias internacionales se harán.
   - Cómo se conservarán y, si procede, cómo y cuando se destruirán.
2. **Crear el fichero** de acuerdo con el procedimiento establecido según sea un fichero de titularidad pública o titularidad privada.
3. **Notificarlo** al Registro de Protección de Datos de Cataluña.
4. **Informar** a las personas afectadas**.**

4.1 La creación, la modificación y la supresión de ficheros

Para poder tratar, ya sea de forma automatizada o no, los datos de carácter personal necesarios para el funcionamiento normal de un centro educativo, antes de iniciar el tratamiento hay que **crear** uno o diversos ficheros.

> **Fichero**
>
> Cualquier conjunto organizado de datos de carácter personal, sea cuál sea la forma o la modalidad de su creación, almacenaje, organización y acceso. Pueden ser ficheros automatizados (en soporte electrónico), no automatizados (en soporte papel), o bien parcialmente automatizados.

Con el paso del tiempo, es posible que determinadas circunstancias obliguen a **modificar** el contenido de los ficheros. Puede ser necesario modificar un fichero porque cambia su responsable, porque se amplían los usos o porque hay que hacer un tratamiento de datos que no se había previsto inicialmente y que puede comportar, además, un cambio en el nivel de medidas de seguridad que hace falta aplicar al fichero. Cualquier cambio que afecte, sustancialmente, al tratamiento de datos configurado inicialmente con la creación del fichero hace necesaria su modificación.

Finalmente, es posible que determinados ficheros se tengan que **suprimir**. Por ejemplo, porque el centro deja de prestar un servicio determinado y, en consecuencia, ya no es pertinente tratar determinados datos personales, o porque los datos que se trataban en un fichero pasan a formar parte de otro, dentro del mismo centro. En este caso, hace falta prever el destino de los datos y valorar si se tiene que derogar el acuerdo de creación por haber quedado sin contenido.

El procedimiento previsto para crear, modificar o suprimir los ficheros varía según si los ficheros son de titularidad pública o privada.

◊ ¿Hay que crear un fichero nuevo si el centro educativo quiere incluir nuevos datos en un fichero ya existente?

No necesariamente. Si los nuevos datos encajan con la finalidad descrita en el fichero y se pueden incluir en alguna de las categorías de datos previstos en la estructura del fichero existente, no hace falta modificarlo ni crear uno nuevo. En cualquier caso, hay que verificar si los nuevos datos requieren elevar el nivel de seguridad.

◊ ¿Se puede añadir una nueva finalidad a un fichero ya existente?

Sí, pero sólo si se trata de una finalidad compatible con la que ya tenía el fichero. En cualquier caso, hay que modificar el fichero y, si procede, informar a las personas afectadas.

4.1.1 Naturaleza de los ficheros de los centros educativos

El RLOPD determina la naturaleza de los ficheros de los centros educativos a partir de la naturaleza pública o privada de la entidad responsable del fichero.

Fichero de titularidad privada

Ficheros los responsables de los cuales sean personas, empresas o entidades de derecho privado, con independencia de quienes tenga la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros los responsables de los cuales sean corporaciones de derecho público no vinculados al ejercicio de las potestades de derecho público que les atribuye su normativa específica.

Fichero de titularidad pública

Ficheros los responsables de los cuales sean órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a estos órganos, las administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las corporaciones de derecho público, siempre que, en este último caso, estén vinculados al ejercicio de las potestades de derecho público que les atribuye su normativa específica.

Los ficheros de centros educativos que tienen como responsable un órgano de una administración pública son ficheros de titularidad pública. En cambio, los ficheros el responsable de los cuales sea un órgano de una entidad de naturaleza privada, con independencia de la procedencia de sus recursos económicos o de la titularidad de su capital, son ficheros de titularidad privada.

Normativa aplicable: art. 2.2 LRJPAC; 5.1.l) y m), 52 y ss. RLOPD.

4.1.2 Procedimiento de creación de los ficheros de titularidad pública

Los ficheros de titularidad pública se tienen que crear, modificar o suprimir mediante una **disposición de carácter general**, que se tiene que publicar en el diario oficial correspondiente y se tiene que notificar a la Autoridad Catalana de Protección de Datos.

Los ficheros de titularidad pública que dependen del Departamento de Enseñanza de la Generalitat de Catalunya se tienen que crear, modificar o suprimir mediante una orden del consejero o consejera de Enseñanza. También se pueden crear, si procede, mediante un decreto. La orden o el decreto se tienen que publicar en el Diario Oficial de la Generalitat de Catalunya.

En el caso de centros educativos que dependen de los entes locales, los ficheros se pueden aprobar por ordenanza o reglamento del pleno de la corporación. En el caso del Ayuntamiento de Barcelona también se pueden aprobar, de acuerdo con su régimen especial, por decreto de la Alcaldía o de la Junta de Gobierno Local. La ordenanza o reglamento se tiene que publicar en el Boletín Oficial de la Provincia.

Contenido:

Los artículos 20 de la LOPD y 54 del RLOPD exigen que la disposición general o acuerdo de creación de nuevos ficheros haga referencia a:

a) La denominación del fichero o tratamiento.

b) La finalidad y los usos previstos.

c) Las personas o los colectivos afectados.

d) El procedimiento de recogida de los datos personales.

e) La procedencia de los datos personales.

f) La estructura del fichero:
   - Tipología de los datos, con descripción detallada de los datos identificativos y, si procede, de los datos especialmente protegidos, y de las restantes categorías de datos.
   - El sistema de tratamiento utilizado en su organización.

g) Las cesiones de datos personales previstos.

h) Las transferencias internacionales de datos personales previstos con indicación, si procede, de los países de destino de los datos.

i) El órgano o los órganos responsables del fichero.

j) Los servicios o las unidades ante las cuales se pueden ejercer los derechos de acceso, rectificación, cancelación y oposición.

k) El nivel de seguridad exigible.

Durante la fase de elaboración de la disposición, el Departamento de Enseñanza tiene que solicitar un informe preceptivo a la Autoridad Catalana de Protección de Datos. Se recomienda adjuntar una copia de la memoria del expediente a la solicitud del informe. En caso de que se creen ficheros de videovigilancia, la memoria tiene que incluir la información requerida en el artículo 10 de la Instrucción 1/2009.

Con respecto a la disposición de **modificación** del fichero, el articulado tiene que indicar qué apartados del fichero se modifican y qué modificaciones se hacen. Se recomienda reproducir, a continuación, el fichero entero con las modificaciones ya incorporadas, con el fin de facilitar la búsqueda a cualquier persona interesada.

La disposición de **supresión** tiene que prever el destino de los datos o, si procede, las previsiones que hay que adoptar para destruirlos.

En relación con la creación, la modificación y la supresión de ficheros, consultar también la Recomendación 1/2011, de la Autoridad Catalana de Protección de Datos sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública.

Normativa aplicable: art. 20.1, 20.3 y 25 LOPD; DF 3ª LACPD; 52 y ss. RLOPD; Orden EDU/316/2010; Orden ENS/125/2011; Orden ENS/59/2014; 9 y 10 Instrucción 1/2009; Recomendación 1/2011; PD 1/2010, PD 15/2010 PD 31/2012, PET 5/2009, PET 8/2011, PET 10/2011.

4.1.3 Procedimiento de creación de los ficheros de titularidad privada

Para crear, modificar o suprimir ficheros de titularidad privada hay libertad de forma. Es suficiente con la voluntad del responsable del fichero (es decir, la decisión de crear unos ficheros destinados a una finalidad concreta, cuando sea necesario para desarrollar las funciones y actividades del centro educativo) y la notificación de este fichero al Registro de Protección de Datos de Cataluña. A diferencia de los ficheros de titularidad pública, no hace falta aprobar ningún acuerdo formal, ni publicarlo.

◊ ¿Los centros educativos concertados tienen que publicar la decisión de crear el fichero?

No hace falta. La notificación de la creación del fichero en el Registro de la Autoridad Catalana de Protección de Datos es suficiente.

4.2 La notificación de los ficheros o tratamientos

La creación o, si procede, la modificación o la supresión de los ficheros de los centros públicos o concertados que ejercen su tarea exclusivamente en el ámbito territorial de Cataluña se tiene que notificar al Registro de Protección de Datos de Cataluña de la Autoridad Catalana de Protección de Datos. Una vez inscritos, la Autoridad los traslada al Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

- El plazo para presentar las solicitudes de inscripción es de 30 días hábiles desde su publicación, en el caso de ficheros de titularidad pública. En el caso de ficheros de titularidad privada se tiene que solicitar antes de crear el fichero.
- Los ficheros se inscriben una vez verificado que cumplen los requisitos establecidos en la LOPD y el RLOPD.
- Transcurrido un mes desde la presentación de la solicitud de inscripción sin que se haya resuelto, el fichero se entiende inscrito a todos los efectos.

En el web de la Autoridad Catalana de Protección de Datos (http://www.apd.cat) encontraréis el software y los formularios de notificación y solicitud de inscripción de los ficheros, así como las instrucciones para llenarlos y enviarlos al Registro, preferentemente de forma telemática.

La inscripción de los ficheros tiene que estar permanentemente actualizada. Cualquier modificación que afecte a su contenido se tiene que notificar a la Autoridad Catalana de Protección de Datos.

◊ ¿A quién corresponde notificar un fichero al Registro de Protección de Datos de Cataluña?

Al responsable del fichero, sin perjuicio que, en el caso de los ficheros públicos, las tareas materiales de notificación se puedan centralizar desde el Departamento de Enseñanza de la Generalitat o, si procede, desde los entes locales.

◊ ¿La Autoridad Catalana de Protección de Datos tiene datos de carácter personal de los alumnos que forman parte del sistema educativo de Cataluña?

No. La notificación del fichero a la Autoridad Catalana de Protección de Datos no comporta la comunicación de los datos personales de las personas afectadas. A raíz de la inscripción, la Autoridad Catalana de Protección de Datos sólo dispone de la información relativa a la descripción de estos ficheros (finalidad, colectivos afectados, tipología de los datos recogidos, responsables delante de los cuales se pueden ejercer los derechos de acceso, rectificación, cancelación y oposición, etc.).

◊ ¿A qué registro tiene que notificar sus ficheros un centro educativo concertado?

Los centros concertados, como entidades que gestionan un servicio público de la Generalitat de Catalunya a través del concierto están incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos, de acuerdo con la LACPD. Por eso, tienen que notificar sus ficheros al Registro de Protección de Datos de Cataluña.

◊ ¿En qué registro se tiene que notificar la modificación de ficheros previamente inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos, pero que ahora están dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos?

Tanto las modificaciones como las supresiones de los ficheros incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos se tienen que tramitar ante el Registro de Protección de Datos de Cataluña, aunque previamente se hayan inscrito en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

Normativa aplicable: art. 26 LOPD; 3. i) y 5.i) LACPD; 55 y s. 130 y 131 RLOPD; Recomendación 1/2011; Res. APDCAT 04.04.2011.

4.3 La información a la persona titular de los datos

El responsable del tratamiento de los datos tiene que garantizar el derecho de información de las personas de las cuales trata los datos personales, con independencia que sea necesario obtener el consentimiento del interesado o se cuente con habilitación legal. La falta de esta información puede comportar un vicio del consentimiento y una infracción en materia de protección de datos.

Contenido

Se tiene que informar a las personas titulares de los datos de forma **expresa, precisa e inequívoca** sobre:

Si los datos se obtienen directamente del titular, antes de la recogida se tiene que informar de:

a) La existencia de un fichero o un tratamiento de datos de carácter personal, la finalidad de la recogida de los datos y los destinatarios de la información.

b) El carácter obligatorio o facultativo de la respuesta a las preguntas que se les planteen.

c) Las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

e) La identidad y la dirección del responsable del tratamiento o, si procede, de su representante.

(No hay que dar la información de los apartados b), c) y d) si se deduce claramente de la naturaleza de los datos o de las circunstancias en que se recogen)

Si los datos se obtienen provenientes de un tercero, en el plazo de tres meses se tiene que informar sobre:

a) El contenido del tratamiento.

b) La procedencia de los datos.

c) La existencia de un fichero o un tratamiento de datos de carácter personal, de la finalidad de la recogida de los datos y de los destinatarios de la información.

d) La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

e) La identidad y la dirección del responsable del tratamiento o, si procede, de su representante.

(No hay que facilitar esta información si se ha informado al interesado anteriormente)

En el anexo 1 de esta Guía se ofrece un modelo de cláusula informativa para los formularios de inscripción a los diferentes servicios escolares (transporte, comedor, guardería, extraescolares, colonias, etc.).

Forma de cumplimiento

El deber información se tiene que hacer efectivo a través de un medio que permita acreditar su cumplimiento y que sea apto para que la persona afectada tenga pleno conocimiento de esta información. De acuerdo con el medio utilizado para la recogida, pueden ser impresos, comunicaciones por escrito, carteles, mensajes pregrabados, otros medios electrónicos, etc.

Cuando se utilizan formularios o impresos para recoger los datos, ya sea en soporte papel o electrónico, la información se tiene que incluir, de forma clara y legible, con independencia que haga falta o no recoger el consentimiento.

Cuando se recogen datos relativos a la ideología, afiliación sindical, religión o creencias, hay que advertir a la persona afectada de su derecho a no facilitar este tipo de datos.

Cuando el tratamiento hace referencia a datos de menores, la información se les debe proporcionar en un lenguaje que les sea fácilmente comprensible.

Excepciones al deber de información

No es necesario cumplir el deber de información en los supuestos siguientes:

- Cuando el cumplimiento del deber de información afecta a la **defensa nacional, la seguridad pública o la persecución de infracciones penales**.
- Cuando los datos no se recogen directamente de su titular, no hay que informar en los supuestos siguientes:
  – Cuando una **ley** prevea expresamente la comunicación.
  – Cuando **ya se haya informado el titular con anterioridad**.
  – Cuando el tratamiento tenga **finalidades históricas, estadísticas o científicas**.
  – Cuando resulte **imposible o exija esfuerzos desproporcionados**, siempre que haya una autorización de la Autoridad Catalana de Protección de Datos.

Cuando los datos procedan de **fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial**, en cada comunicación que se dirija al interesado el responsable del fichero o tratamiento le tiene que informar del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que lo asisten.

◊ ¿Cuando no es necesario el consentimiento, hay que informar igualmente?

Sí. El deber de información se tiene que cumplir en todos los casos, salvo alguna de las excepciones previstas en la LOPD.

◊ ¿Hay que incluir la cláusula informativa en todos los correos electrónicos que envía el centro a los alumnos o a sus padres o tutor?

No, no es obligatorio si ya se informó en el momento de la recogida de los datos. Pero sí que puede ser recomendable incluirla en los correos en que se solicita la actualización o complementación de los datos, así como tenerla a disposición de los interesados a través del web. Así, las personas que se relacionan con el centro educativo saben dónde están sus datos, el tratamiento que se hace, quién es el responsable y cómo pueden ejercer sus derechos.

◊ ¿Quién tiene que informar cuando se ha producido una cesión de datos personales?

La obligación de informar de la cesión es del cesionario sin perjuicio que si para hacer la cesión hace falta el consentimiento de las personas afectadas, corresponde al cedente informar antes de obtener el consentimiento.

◊ ¿Si un centro educativo concertado contrata una empresa para hacer estudios psicopedagógicos quien tiene que cumplir con el deber de información?

En principio, la obligación de informar a las personas afectadas corresponde al responsable del tratamiento. Si el responsable del tratamiento no lo ha hecho, la empresa encargada del tratamiento tiene que informar antes de iniciar el estudio.

◊ ¿Hay que informar a los padres de un menor si se comunican datos relativos a una situación de riesgo a los servicios sociales?

No. Dado que la Ley 14/2010, del 27 de mayo, de los derechos y las oportunidades en la infancia y la adolescencia, prevé la obligación de hacer esta comunicación (art. 100), no es necesario que el centro informe a los padres del menor.

◊ ¿Debe informarse de la utilización de una plataforma facilitada por un tercero (encargado del tratamiento) para la gestión académica y administrativa del centro educativo?

A pesar que la normativa de protección de datos no lo exige de manera expresa, en la medida que la utilización de estas herramientas tecnológicas facilitadas por terceros conlleva la recogida y tratamiento de datos personales de alumnos, padres o tutores legales y maestros, se recomienda informarles a cerca de las circunstancias en las que se trataran sus datos (identidad del proveedor de los servicios, finalidad del tratamiento, condiciones del tratamiento, etc.).

Normativa aplicable: art. 5, 24 LOPD; 5.p) LACPD; 13.3 RLOPD; CNS 38/2009.

5 Obligaciones durante el tratamiento de los datos

Los principios, las obligaciones y las garantías previstas por la normativa de protección de datos se tienen que tener en cuenta no sólo en el momento de la recogida de los datos, sino también durante cualquier fase del tratamiento

Las personas afectadas (alumnos, familiares, personal del centro, etc.) disponen de una serie de garantías encaminadas a asegurar la adecuación del tratamiento de sus datos personales a la normativa vigente, que se tienen que aplicar durante la recogida, el almacenaje, la utilización o la comunicación de los datos de carácter personal e, incluso, después de que finalice la relación jurídica.

Estas garantías son:

- El deber de secreto.
- El mantenimiento y la actualización de los datos personales.
- Los derechos de acceso, rectificación, cancelación y oposición.
- La implementación de medidas de seguridad..

5.1 El deber de secreto

Para desarrollar sus funciones, los centros educativos necesitan la colaboración no sólo de los profesores, sino también de diferentes profesionales, psicólogos, pedagogos, logopedas, maestros de educación especial, educadores sociales y personal sanitario que presta sus servicios en el centro. Los centros también cuentan con personal administrativo y otros servicios auxiliares, como el mantenimiento o el comedor. Todos ellos acceden o pueden acceder en algún momento a los sistemas de información o documentación que contienen datos de carácter personal de los alumnos.

El responsable del fichero y todas estas personas que pueden intervenir en cualquiera de las fases del tratamiento de datos de carácter personal están obligados a guardar secreto respecto de estos datos. En este sentido, la LOE establece que el profesorado y el resto del personal que, para ejercer sus funciones, acceda a

datos personales y familiares o que afecten el honor y la intimidad de los menores o sus familias queda sujeto al deber de sigilo.

Para garantizar el cumplimiento de este deber, en una relación jurídica que comporte el tratamiento de datos de carácter personal, es recomendable incorporar y definir esta obligación en los contratos laborales, en los protocolos internos, en las actividades formativas y en las regulaciones específicas que recogen los derechos y las obligaciones de las partes. Esta obligación subsiste incluso una vez finaliza la relación con el responsable.

El cumplimiento del deber de secreto es todavía más importante en un ámbito como el educativo, donde a menudo se puede tratar información que tiene que ser especialmente protegida. Es el caso de la información obtenida por las áreas de orientación, psicólogos, pedagogos, logopedas, educación especial y educadores sociales, y que puede incluir diagnósticos, valoraciones y dictámenes profesionales sobre el estado de salud física o psíquica de los alumnos o valoraciones sobre su vida personal y familiar.

Este deber de secreto se tiene que diferenciar del secreto profesional relacionado con determinadas profesiones concretas. El deber de secreto afecta a cualquier persona que tenga acceso al tratamiento de datos de carácter personal.

◊ **¿La información sobre los alumnos de que dispone el centro tiene que estar disponible para todos los maestros y personal del centro en carpetas de uso compartido?**

Los maestros están legitimados para acceder a los expedientes académicos de sus alumnos con finalidades académicas. Ahora bien, este acceso no puede ser indiscriminado, es decir, no puede ser abierto a todo el profesorado del centro. Cada profesor tiene que tener acceso sólo a los datos de los alumnos respecto de los cuales tiene que intervenir y no está justificado el acceso a los datos del resto de alumnos.

◊ **¿Hay que establecer alguna previsión específica respecto de los estudiantes universitarios en prácticas en el centro educativo?**

Se recomienda firmar un acuerdo de confidencialidad entre el estudiante en prácticas y el centro educativo, con respecto a la información de terceras personas a la cual puedan tener acceso con motivo de las prácticas.

Normativa aplicable: art. 10 LOPD; ap. 3 DA 23ª LOE; 83 RLOPD.

5.2 La comunicación o cesión de datos personales a terceros

Para ejercer sus funciones, tanto los centros educativos públicos como los concertados, pueden tener que comunicar a un tercero los datos personales que tratan en sus ficheros. En estos casos, hay que sujetarse al régimen de cesiones o comunicaciones previsto en la LOPD.

Cesión o comunicación de datos personales

Cualquier revelación de datos personales efectuada a una persona diferente a la persona afectada.

Tercero

Persona física o jurídica, pública o privada, u órgano administrativo diferente del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

También pueden ser terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

5.2.1 Requisitos

Para que una cesión o comunicación sea legítima, tiene que cumplir **dos requisitos**:

1) Que responda al cumplimiento de **finalidades** directamente relacionadas con las funciones legítimas del cedente y del cesionario.

2) Que se haya obtenido el **consentimiento previo** de la persona afectada o que concurra alguna de las circunstancias siguientes:

- Esté autorizada por una **norma con rango de ley** o una norma de derecho comunitario.
- Se trate de datos recogidos de **fuentes accesibles al público**.
- Responda a la aceptación libre y legítima de **una relación jurídica** que implique necesariamente la comunicación de datos al tercero, para su cumplimiento, desarrollo y control, siempre que se limite a la finalidad que la justifica. Esta relación jurídica puede ser de carácter laboral, administrativa, asociativa, corporativa o contractual.
- El destinatario sea el **Defensor del Pueblo, el Ministerio Fiscal, los jueces y tribunales o el Tribunal de Cuentas** y las **instituciones autonómicas análogas**, en el ejercicio de sus funciones.
- Se comuniquen datos relativos a la salud para solucionar una urgencia o para hacer **estudios epidemiológicos** en los términos que establezca la legislación sanitaria.
- El tratamiento o la cesión tengan por objeto satisfacer un **interés legítimo** del responsable del tratamiento o del cesionario amparado por estas normas, siempre que no prevalezca el interés o los derechos y las libertades fundamentales de los interesados.

La comunicación de datos **entre administraciones públicas** está específicamente regulada en el artículo 21 de la LOPD, que prevé la posibilidad de ceder datos a otra administración pública sin disponer del consentimiento de las personas afectadas cuando:

- Se comunican para ejercer las mismas competencias.
- Se comunican para ejercer competencias que versan sobre la misma materia.

- La comunicación tiene por objeto el tratamiento de los datos con finalidades históricas, científicas o estadísticas.
- Una administración pública las obtiene o elabora con destino a otra administración.

De acuerdo con la LOE, la cesión de los datos necesarios para el sistema educativo, incluidos los de carácter reservado, se tiene que hacer preferentemente por vía telemática y está sujeta a la legislación en materia de protección de datos de carácter personal. Las condiciones mínimas las tiene que acordar el Gobierno con las comunidades autónomas, en el seno de la Conferencia Sectorial de Educación.

Normativa aplicable: art. 1, 3.i), 11, 21, 27 y 28 LOPD; 7.f) Directiva 95/46/CE; ap. 2 y 4 DA 23ª LOE; 50.4 LE; 2.2, 5.1.c) y r), 7.1.c), 10 RLOPD.

5.2.2 Comunicaciones de datos para finalidades académicas

La LOE habilita la recogida y el tratamiento de los datos de los alumnos que sean estrictamente necesarios para la función docente y orientadora. También habilita la cesión en el centro educativo en el cual se haya inscrito un alumno de los datos procedentes del centro donde haya sido escolarizado anteriormente.

Eso puede incluir determinadas comunicaciones o revelaciones de información al resto de miembros del grupo del alumno que resultan estrictamente necesarias para la actividad docente, pero conviene tener presente que no habilita cualquier cesión.

◊ ¿Se pueden colgar las listas de los alumnos en las puertas de las clases durante todo el curso?

Aparte de la posibilidad de colgar las listas los primeros días de curso con la finalidad que alumnos y padres puedan localizar cuál es su clase, es recomen-

dable que a partir de entonces, si tienen que continuar expuestas, permanezcan colgadas sólo en el interior de las aulas. Para informar del carácter interno de estas listas se puede incluir una advertencia en este sentido.

◊ ¿El centro educativo, tiene que comunicar a los padres o al tutor los datos psicopedagógicos que constan en el expediente de su hijo?

La comunicación a los padres de los datos académicos y psicopedagógicos que guardan relación con la formación de hijos menores de edad no emancipados estaría amparada por el artículo 11.2.a) de la LOPD de acuerdo con el artículo 236 CCC y 154 del CC.

◊ ¿Aparte de los padres, el resto de familiares pueden acceder a los datos del menor?

No. En principio el resto de familiares sólo pueden acceder si tienen atribuida la tutela del menor o con el consentimiento de los afectados.

◊ ¿Hace falta el consentimiento del maestro para comunicar su correo electrónico profesional a un padre que lo solicita?

La comunicación de la dirección de correo profesional del maestro a fin de que unos padres puedan ponerse en contacto, por motivos relacionados con el seguimiento de la actividad de su hijo, está amparada tanto por el artículo 11.2.c) LOPD como por el art. 2.2 RLOPD.

◊ ¿Se puede difundir en la revista del centro educativo información sobre incidentes o medidas disciplinarias en el ámbito del centro?

Conviene limitar estas publicaciones a los supuestos en que se trata de informaciones veraces y de relevancia pública, en la que la libertad de información tiene que prevalecer sobre la privacidad de las personas. En cualquier caso, siempre que sea posible, conviene anonimizar la información.

◊ ¿El centro educativo puede facilitar a un museo los datos de los alumnos que participan en una visita?

En principio, conviene evitar facilitar los datos sobre los alumnos, a menos que sean estrictamente necesarios para hacer la visita. En este caso, se puede utilizar el formulario donde se pide autorización a los padres o al tutor para participar en la salida para pedir el consentimiento para comunicar los datos de los alumnos al museo.

◊ ¿Un centro educativo puede facilitar datos personales a alguien que lo solicita por teléfono?

La comunicación de datos por teléfono no permite, en principio, comprobar la identidad de quién lo solicita. Por eso, en los casos en que las circunstancias hagan necesario facilitarlos, hay que utilizar algún sistema que permita acreditar la identidad, como que el interlocutor tenga que facilitar alguna información que sólo puedan conocer las partes implicadas.

En cambio, sí que se puede facilitar mediante el teléfono identificado previamente como teléfono de contacto por los padres o tutor del alumno de que se trate.

◊ ¿Qué medidas ha de tomar el centro educativo a la hora de enviar correos electrónicos dirigidos de forma masiva a todos los padres?

Conviene utilizar la opción de copia oculta para evitar la divulgación indebida de la dirección de correo del resto de padres incluidos a la comunicación.

◊ ¿Un padre o una madre puede solicitar las calificaciones académicas de su hijo al centro educativo?

Si los alumnos son menores de edad no emancipados, los padres que tienen la patria potestad, o si procede el tutor, tienen derecho a solicitar las calificaciones académicas de su hijo. En cambio, si es mayor de edad o está emancipado, el centro educativo sólo tiene que comunicar las calificaciones al hijo.

Normativa aplicable: ap. 2 y 4 DA 23ª LOE; art. 50.4 LE.

5.2.3 Publicaciones en el web del centro educativo

La publicación de información relativa a los alumnos, a los profesores o a sus familias en el web del centro educativo constituye una comunicación de datos de carácter personal, dado que permite que terceras personas puedan tener conocimiento de la misma. Y eso incluye no sólo personas que forman parte de la comunidad educativa, sino también terceras personas que no tienen ningún tipo de relación. Por lo tanto, cuando se quiera publicar información de carácter personal en el web, hay que disponer del consentimiento de los padres o tutor, o de los mismos alumnos afectados si son mayores de 14 años, o que concurra algún otro de los supuestos a que nos hemos referido en este apartado de la Guía.

Por eso, y a menos que se cuente con el consentimiento específico de las personas afectadas u otra habilitación, conviene que en este espacio se facilite información sobre el centro educativo, su actividad y su organización, pero no información personal sobre los alumnos.

En cualquier caso, hay que velar para que la información que se publica sea exacta y actualizada, establecer los mecanismos adecuados de revisión y aplicar las medidas de seguridad apropiadas con respecto a la identificación de las personas que pueden actuar como administradoras del web.

◊ **¿Se pueden publicar en el web del centro los nombres y los datos de contacto profesional del tutor, profesores y otros responsables del centro?**

El artículo 2.2 del RLOPD puede permitir la comunicación de estos datos. Ahora bien, dado que los destinatarios de esta información tienen que ser los miembros de la comunidad educativa, es recomendable publicarlo exclusivamente en la intranet.

◊ ¿Se pueden publicar en el web imagenes o vídeos de los alumnos haciendo diferentes actividades en el centro?

La publicación en Internet de estas imágenes de los alumnos es una comunicación de datos y por lo tanto, requiere el consentimiento de los padres o tutor o del mismo alumno afectado, si es mayor de 14 años. Ahora bien, se pueden difundir imágenes en que los alumnos no resulten reconocibles sin esfuerzos desproporcionados o cuando se trate de una imagen captada en un acto público (p. ej. fiestas del centro abiertas a familiares y amigos) y en la cual la imagen de la persona aparezca como meramente accesoria.

◊ ¿Es suficiente obtener el consentimiento del alumno o de sus padres o tutor una única vez, o hay que obtenerlo cada vez que se quiera hacer una fotografía y publicarla?

Con la obtención del consentimiento para una finalidad concreta una sola vez puede ser suficiente. En cualquier caso, en el momento de pedir el consentimiento se debe informar a las personas afectadas de manera clara sobre la finalidad y el periodo de validez de la autorización.

◊ ¿Hay que contar con el consentimiento para difundir imágenes de alumnos en el web del centro si las imágenes están difuminadas o se trata de una fotografía colectiva en que los alumnos no son identificables?

No. Al no ser identificable, sin esfuerzos desproporcionados, la persona afectada, la imagen no tiene la consideración de dato de carácter personal. En consecuencia, la normativa de protección de datos no es de aplicación.

Normativa aplicable: art. 3.a) LOPD; 8.2.c) LO 1/1982; 2.2, 5.1.o) RLOPD; Recomendación 1/2008; CNS 37/2013.

5.2.4 Publicaciones en la intranet o blogs del centro educativo o en el tablón de anuncios

En caso de que los datos personales se publiquen en la intranet o blogs del centro educativo, aunque en este caso el número de personas que acceden se limita a las personas de la comunidad educativa, también nos encontramos ante una comunicación. Por eso, también se tiene que contar con el consentimiento de las personas afectadas o con otra habilitación.

Estos espacios, en los cuales se accede previa identificación y autenticación, son adecuados para difundir información sobre la actividad ordinaria o extraordinaria del centro y para difundir información entre los miembros de la comunidad educativa. Ahora bien, cuando se incluya información sobre la actividad o la evolución de alumnos concretos la comunicación se tiene que hacer a través de canales de comunicación personalizados que, previa identificación y autenticación, permitan acceder sólo a la información personal relativa a cada usuario.

Puede ser recomendable segmentar la información que se ofrece en estos espacios según los diferentes grupos existentes en el centro (grupo, curso, etapa, etc.)

Las consideraciones que se hacen sobre la intranet son extensibles también a los tablones de anuncios de los centros, porque en principio tienen el acceso limitado a las personas que forman parte de la comunidad educativa.

◊ ¿Se puede difundir en la intranet una relación de los alumnos de la clase con una fotografía?

La incorporación de un alumno a una clase comporta que el resto de miembros puedan tener conocimiento tanto de su imagen como de su identidad. Ahora bien, conviene que el acceso quede limitado a los alumnos y a los padres que formen parte del grupo, y que previamente se informe a los padres para que, si lo desean, puedan hacer uso del derecho de oposición.

◊ ¿Las calificaciones de los alumnos se pueden difundir en la intranet?

Las calificaciones se pueden difundir a través de la intranet siempre que se garantice que sólo tiene acceso el alumno de qué se trate o, en el caso de menores no emancipados, sus padres.

◊ ¿Y en los tablones de anuncios del centro?

No. A diferencia de lo que sucede en el ámbito universitario, en este caso no es posible porque a estos mostradores puede acceder cualquier otra persona de la comunidad educativa y no hay una norma legal que lo habilite.

Normativa aplicable: art. 6.4 LOPD; Recomendación 1/2008; CNS 41/2011.

5.2.5 Comunicaciones de datos para actividades extraacadémicas

Los datos que el centro educativo recoge relativos a sus alumnos se pueden tratar con finalidades relacionadas con el desarrollo de las actividades propias de la función educativa. Hay que evitar la comunicación de estos datos con finalidades diferentes.

◊ ¿El centro educativo puede facilitar a unos padres las fechas de nacimiento de todos los niños de su clase, para organizar los aniversarios?

No. Hace falta el consentimiento de los padres o tutor.

◊ **¿El centro educativo está legitimado para comunicar el correo electrónico de padres y alumnos a una editorial de revistas infantiles, para ofrecerles suscripciones en condiciones ventajosas?**

No. Se trata de una finalidad incompatible con aquélla para la cual se recogieron los datos y por lo tanto, hay que contar con el consentimiento de padres o tutor.

◊ **¿Si se ha autorizado el centro educativo para utilizar las imágenes de un alumno para informar de las actividades escolares, las imágenes se pueden utilizar también para hacer publicidad del centro?**

Sólo pueden utilizarse con esta finalidad si en el momento de pedir el consentimiento se informó sobre esta posibilidad de uso.

◊ **¿El centro educativo puede facilitar a los padres los datos de contacto del resto de los padres de la clase, para poder comunicarse para organizar actividades extraescolares u otras iniciativas de participación en la vida escolar?**

No. No hay ninguna norma legal que habilite esta comunicación. Por lo tanto, hace falta el consentimiento de los otros padres.

5.2.6 Comunicaciones de datos para finalidades administrativas del centro

Más allá de la actividad estrictamente académica, el funcionamiento del centro educativo comporta también actividades administrativas relacionadas tanto con el proceso de preinscripción y matriculación de los alumnos como con la gestión de personal, la gestión de proveedores o la contratación de seguros.

◊ ¿Se pueden colgar las listas de los alumnos admitidos en el proceso de preinscripción en el tablón de anuncios del centro? ¿Qué datos pueden figurar?

Al tratarse de un procedimiento de concurrencia competitiva, el artículo 59.6.b) de la LRJPAC habilita para que la convocatoria del procedimiento establezca el tablón de anuncios o medio de comunicación donde se harán las publicaciones sucesivas.

En caso de que la convocatoria no especifique otros medios de comunicación, la publicación en el tablón de anuncios del centro puede ser suficiente.

A menos que la convocatoria establezca otra cosa, puede constar el nombre y apellido de los alumnos solicitantes y los admitidos al centro, así como la puntuación baremada que hayan obtenido.

◊ ¿Los padres de un niño que no ha resultado admitido en el proceso de preinscripción en un centro pueden acceder a la información alegada por los admitidos?

El ciudadano que ha formado parte de un procedimiento selectivo concurrencial, en este caso por medio de la preinscripción de su hijo en un centro educativo, tiene la consideración de persona interesada en aquel procedimiento administrativo y, como tal, puede tener acceso a los datos de las personas admitidas (art. 35 LRJPAC).

Si el acceso tiene por objetivo conocer el domicilio que han hecho constar otros candidatos, para comprobar si ha habido fraude en la puntuación obtenida por el empadronamiento, el acceso es necesario para que el ciudadano pueda ejercitar su derecho de defensa.

Los datos contenidos en los expedientes de preinscripciones, relativos a nombre, apellidos y al empadronamiento de los alumnos que han accedido a un centro educativo, no se pueden considerar datos íntimos, si bien el mismo expediente puede contener datos relativos a la intimidad de las personas como circunstancias personales o familiares. En este caso, el órgano responsable de estos datos puede otorgar el acceso al dato relativo al domicilio sin necesidad de dar a conocer los otros datos que conforman el expediente administrativo y que se pueden considerar datos íntimos.

◊ **¿El Departamento de Enseñanza puede solicitar información a un ayuntamiento sobre la inscripción en el padrón municipal de personas que han participado en el proceso de preinscripción, para contrastar la veracidad de los datos aportados?**

Sí. El artículo 50.4 de la LE establece que la Administración educativa puede reclamar la colaboración de otras administraciones para contrastar la veracidad de los datos aportados en los procesos de admisión.

◊ **¿Un centro educativo puede comunicar datos de los alumnos a la empresa aseguradora con quien tiene contratada el seguro escolar?**

Sí, dado que si el centro educativo ha establecido un seguro colectivo de este tipo, la incorporación del alumno en el centro comporta que pase a tener la condición de asegurado. La comunicación de datos es necesaria para desarrollar esta relación jurídica (art. 11.2.c) LOPD). Eso, sin perjuicio que el centro tiene que informar los alumnos o representantes sobre esta comunicación.

◊ **¿El centro puede facilitar los datos de su personal a una entidad financiera con la finalidad de pagar la nómina?**

Sí, dado que la comunicación de datos es necesaria para desarrollar la relación laboral (art. 11.2.c) LOPD).

◊ **¿Se tienen que publicar los nombramientos de personal docente en procesos de provisión derivados de la necesidad de trasladar, como medida de protección, a una docente víctima de violencia de género?**

No. El artículo 126 de la LE prevé que en estos procesos relacionados con la protección de las víctimas de la violencia machista se tiene que proteger especialmente la intimidad de la víctima y también sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda y custodia.

Normativa aplicable: art. 11.2.c) LOPD; art. 50.4 LE; art. 31, 35.a) y 59.6.b) LRJPAC; CNS 31/2010, CNS 29/2011, CNS 19/2013, CNS 23/2013.

5.2.7 Comunicaciones a administraciones públicas

En otros casos, la comunicación de datos puede estar relacionada con el ejercicio de competencias administrativas diferentes a la función educativa. En estos casos, y a menos que se cuente con el consentimiento de las personas afectadas, hace falta que una ley habilite la comunicación de forma específica.

◊ **¿Un centro educativo puede comunicar datos de salud de los alumnos a una administración pública, para hacer un estudio estadístico?**

Si un centro educativo dispone de datos de salud de sus alumnos y una administración pública los requiere para hacer un estudio estadístico, el centro puede comunicar estos datos previa disociación, es decir, evitando comunicar los datos que permitan identificarles.

◊ **¿Las situaciones de riesgo o de desamparo de menores que se detecten en el centro educativo se pueden comunicar a los servicios sociales?**

Sí. El artículo 100 de la Ley 14/2010, del 27 de mayo, de los derechos y las oportunidades en la infancia y la adolescencia, establece que los ciudadanos que tienen conocimiento de la situación de riesgo o desamparo en que se encuentra un niño o adolescente tienen el deber de comunicarlo a los servicios sociales básicos, especializados o del departamento competente en materia de protección de los niños y los adolescentes, lo antes posible. Este mismo artículo prevé que se tiene que garantizar la confidencialidad de la identidad de la persona que lo ha denunciado.

◊ **¿El centro educativo tiene que atender los requerimientos de información sobre los alumnos que haga la policía?**

El centro educativo, como responsable del fichero de los datos de los alumnos tiene que atender la petición de información concreta y específica de la policía si se acredita que se hace para prevenir un peligro real para la seguridad pública o para la represión de infracciones penales.

Si la información requerida es especialmente protegida (art. 7 LOPD), sólo se tiene que facilitar si es absolutamente necesaria en el marco de una investigación concreta.

◊ **¿El centro educativo tiene que facilitar los datos de los alumnos al personal del Catsalut que se desplaza al centro para vacunar a los alumnos?**

A menos que se trate de una vacunación obligatoria, hay que contar con el consentimiento de los padres o tutor.

◊ **¿En este caso, cómo tienen que prestar el consentimiento los padres? ¿Es suficiente con que el alumno lleve al centro el libro de vacunaciones?**

No, al tratarse de datos de salud, hace falta que el consentimiento sea expreso.

◊ **¿Puede un ayuntamiento ceder datos del padrón municipal de habitantes a la administración educativa, para que pueda recordar a los padres de niños menores de una determinada edad los periodos de preinscripción escolar?**

Sí. El artículo 16.3 de la LRBRL habilita la cesión de los datos del padrón a otras administraciones públicas en que el dato relativo al domicilio o la residencia resulte relevante.

◊ **¿Puede una empresa que presta el servicio municipal de danza comunicar los datos recogidos de los alumnos al Ayuntamiento titular del servicio?**

Sí, si en el momento de la recogida se informó a las personas sobre la titularidad municipal del servicio, o bien, de acuerdo con lo que establece el artículo 11.2.c) LOPD, en la medida que se trata de información que se tiene que comunicar a la entidad municipal para ejercer las funciones de control sobre el servicio que tenga atribuidas.

Normativa aplicable: 22 LOPD; 100 Ley 14/2010; CNS 27/2011, CNS 40/2012, CNS 14/2014, CNS 16/2014.

5.3 El encargado del tratamiento

Los centros educativos, como responsables de los ficheros, pueden encargar a terceras personas o entidades un tratamiento de datos personales o una actividad que comporte el tratamiento de datos de carácter personal, como la organización de actividades extraescolares, el servicio de autocar, el servicio de comedor u otros servicios externalizados (natación, asesoría contable y laboral, destrucción de papel, plataforma o software de gestión del centro educativo, etc.). En este caso, hay que tener presente la figura del encargado del tratamiento.

> **Encargado del tratamiento**
>
> Persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.
>
> También pueden ser encargados del tratamiento los entes sin personalidad jurídica que actúan en el tráfico como sujetos diferenciados.

En otros casos, puede ser el mismo centro educativo quien actúe como encargado del tratamiento, a consecuencia del encargo que haya recibido para ejercer determinadas funciones o actividades por cuenta de otras entidades, que serían las responsables del fichero.

En estos casos, cuando el acceso del tercero a los datos de carácter personal es necesario para prestar el servicio, no se considera comunicación de datos si la relación entre el responsable del tratamiento y el encargado del tratamiento se regula en un contrato o acuerdo de encargo, por escrito o en alguna otra forma que permita acreditar la celebración y el contenido, el cual tiene que establecer:

a) Que únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

b) Que no utilizará los datos con una finalidad diferente de la predeterminada en el contrato.

c) Que no comunicará los datos, ni siquiera para conservarlos, a terceras personas.

d) Las medidas de seguridad.

Si no se establece este contrato o acuerdo, el acceso del tercero a los datos constituye una cesión y se tiene que someter a los requisitos establecidos en la normativa de protección de datos para las cesiones.

En los contratos sometidos a la legislación de contratos del sector público, el acuerdo o contrato de encargo tiene que constar necesariamente **por escrito**.

Si el encargado del tratamiento incumple alguna de estas obligaciones, se considera como responsable del tratamiento y le son imputables, personalmente, las infracciones que ha cometido.

Una vez cumplida la prestación contractual, y de acuerdo con las indicaciones del responsable del tratamiento, los datos se tienen que **destruir o restituir** al responsable del tratamiento o al encargado que haya designado.

- En los casos en que haya una previsión legal que exija la conservación, se tienen que restituir al responsable garantizando la conservación.
- El encargado puede conservar los datos bloqueados, para atender posibles responsabilidades.

Para el análisis de esta figura con más detalle, se puede consultar la Recomendación 1/2010.

◊ ¿La empresa contratada para gestionar el servicio de comedor escolar es un encargado del tratamiento?

Sí, si la empresa tiene que acceder a datos personales de los alumnos, por ejemplo para identificar los que tienen que seguir una dieta especial, y el responsable del fichero y la empresa han firmado un acuerdo con las previsiones establecidas en el artículo 12.2 LOPD.

Ahora bien, si no hace falta que la empresa trate datos personales, por ejemplo porque los monitores u otro personal del mismo centro son los que verifican que los alumnos estén inscritos en el servicio y, si procede, les reparten los menús especiales, la empresa no tiene la consideración de encargado del tratamiento.

◊ ¿Si se ha establecido el acuerdo de encargo del tratamiento, a qué datos puede acceder el personal encargado del servicio?

El personal de la empresa puede acceder a los datos que establezca el acuerdo de encargo, que no pueden ser más de los estrictamente necesarios para prestar el servicio (identificación del alumno, curso, turno de comedor, dietas especiales, etc.)

◊ ¿Si el centro ya había contratado un tercero para prestar servicios que comportan el acceso a datos personales y no había incluido las cláusulas previstas en el artículo 12 LOPD, puede incorporarlos con posterioridad?

Sí. El centro puede firmar un anexo o un acuerdo complementario en el contrato con las previsiones establecidas en el artículo 12.2 LOPD.

◊ ¿La empresa contratada para prestar el servicio de transporte escolar también es un encargado del tratamiento?

Si el centro le facilita información sobre la identificación de los alumnos usuarios del servicio, turnos, paradas que utilizarán, etc., la empresa que presta el servicio de transporte tiene la consideración de encargado del tratamiento si se establece el acuerdo de encargo a que se refiere el artículo 12 LOPD. De lo contrario, el acceso a esta información tiene la consideración de cesión o comunicación de datos.

◊ ¿Hay que firmar un contrato de encargo del tratamiento con la empresa que hace la limpieza del centro?

En las prestaciones de servicios por terceros que no tengan que comportar acceso a datos de carácter personal, como los contratos de limpieza -o, por ejemplo, los de mantenimiento general-, no hay un encargo del tratamiento.

En estos casos, el contrato tiene que incluir expresamente la prohibición de acceder a datos personales y la obligación de guardar secreto respecto de los datos en que accidentalmente se tenga acceso.

Además, conviene dar información al personal que interviene en la prestación de servicios sobre los riesgos que puede generar su actividad para el sistema de información, así como sobre otros aspectos como el sistema de control de los accesos físicos, el proceso de eliminación de documentos y soportes o las condiciones de ventilación y refrigeración necesarias para que los equipos funcionen correctamente.

Por otra parte, es recomendable incluir en el contrato de prestación de servicios la obligación de la entidad adjudicataria de poner en conocimiento del responsable del fichero o tratamiento, de forma inmediata, cualquier incidencia que se produzca durante la prestación del servicio que pueda afectar a la integridad o la confidencialidad de los datos de carácter personal tratados por la entidad adjudicadora.

◊ ¿Los monitores que se contratan para hacer las actividades extraescolares tienen la condición de encargados del tratamiento?

En principio, si se establece una relación laboral del centro educativo con el monitor, éste no tiene la condición de encargado del tratamiento, sino que forma parte del mismo centro como el resto de trabajadores.

Cada año se entrega a la empresa que presta el servicio de piscina un listado actualizado de los alumnos que hacen uso de este servicio. ¿Hay que firmar un contrato o acuerdo de encargo cada año?

Sólo hay que firmar un solo acuerdo o contrato, si las condiciones del encargo no varían sustancialmente.

◊ **¿Si el centro educativo contrata una empresa para la recogida selectiva y destrucción de papel, hay que incluir alguna previsión específica desde el punto de vista de la normativa de protección de datos?**

El centro tiene que firmar el acuerdo o contrato de encargo del tratamiento con esta empresa, dado que para ejercer las funciones encomendadas trata la información personal que puede contener la documentación.

◊ **¿La utilización de servicios de "cloud storage" por el centro educativo exige un acuerdo de encargo del tratamiento?**

Sí, siempre que en los documentos almacenados por el centro educativo consten datos de carácter personal. La utilización de servicios de almacenamiento de la información en la "nube" implica que un tercero (la empresa proveedora) trate datos personales de los ficheros o de los sistemas de los cuales es responsable el centro educativo. Dicho tratamiento se considera un acceso a datos personales por cuenta de terceros y exige un acuerdo de encargo del tratamiento. De lo contrario, se considera una cesión o comunicación de datos.

◊ **¿La empresa contratada para la gestión de una plataforma de gestión académica de contenidos digitales y de comunicación con las familias es un encargado del tratamiento?**

Sí, siempre que, para la prestación de los servicios ofrecidos, la empresa trate datos personales de los cuales es responsable el centro educativo. Debe establecerse el acuerdo de encargo previsto en el artículo 12 LOPD. En caso contrario, el acceso a esta información por la empresa que presta estos servicios tendría consideración de cesión o comunicación de datos.

En estos casos, ¿es necesario establecer en el acuerdo o contrato con la empresa que presta dichos servicios alguna previsión específica desde el punto de vista de la normativa de protección de datos?

Sí. Debe firmarse un contrato o acuerdo con la empresa proveedora de la plataforma o software de gestión del centro educativo con las previsiones establecidas en el artículo 12.2 de la LOPD.

Por otro lado, es importante establecer el destino de la información migrada por el centro educativo o recogida por la misma plataforma una vez finalice

la prestación contractual. Es decir, si estos datos (y, si procede, el soporte en el que consten) deben ser destruidos, devueltos al centro educativo o bien a otro encargado que éste haya designado.

Asimismo, si la empresa proveedora almacena los datos personales en servidores ubicados fuera del Espacio Económico Europeo y se exige la autorización del Director de la Agencia Española de Protección de Datos para la transmisión internacional de los datos, se recomienda incluir en el acuerdo las cláusulas contractuales tipo establecidas por la Comisión Europea en la Decisión 2010/87/UE de 5 de febrero de 2010.

Normativa aplicable: art. 3. g), 9 y 12 LOPD; DA 26 TRLCSP; 5.1.i), 20 y ss., 82 RLOPD; Recomendación 1/2010; CNS 25/2010, CNS 38/2009.

5.4 Transferencias internacionales de datos

La normativa de protección de datos establece una regulación específica para las transferencias internacionales de datos, es decir, para todas las comunicaciones de datos con un destinatario situado fuera del territorio del espacio económico europeo.

Estas previsiones pueden ser de aplicación en supuestos en qué los centros educativos tengan que comunicar datos, por ejemplo en relación con alumnos que cursan parte de sus estudios en otro país que no forme parte de la Unión Europea o que haga estancias organizadas por el centro educativo en alguno de estos países.

Este tipo de comunicaciones requieren que la legislación del país destinatario proporcione un nivel adecuado de protección. De lo contrario, hay que obtener autorización del director o la directora de la Agencia Española de Protección de Datos.

No obstante, la normativa establece una serie de supuestos en que se permite la transferencia internacional de datos sin necesidad de autorización:

a) Cuando resulta de la aplicación de un tratado o convenio del cual España sea miembro.

b) Cuándo tiene por objeto dar o solicitar auxilio judicial internacional.

c) Cuando es necesaria para el diagnóstico o la asistencia sanitaria.

d) Cuando hace referencia a transferencias dinerarias.

e) Cuando la persona afectada ha dado su consentimiento inequívoco.

f) Cuando es necesario para ejecutar un contrato entre la persona afectada y el responsable del fichero, o entre éste último y un tercero, cuando es en interés de la persona afectada.

g) Cuando es necesaria o legalmente exigida para salvaguardar un interés público.

h) Cuando se requiere para ejercer un derecho dentro de un procedimiento judicial.

i) Cuando la petición la efectúa una persona con un interés legítimo desde un registro público.

j) Cuando tiene como destino un estado respecto del cual la Comisión Europea ha declarado que garantiza un nivel de protección adecuado.

◊ ¿La utilización de los servicios ofrecidos por empresas que operan en la "nube" conlleva una transferencia internacional de datos personales por parte del centro educativo?

Sí, si los servidores que almacenan los datos personales de los cuales es responsable el centro educativo se encuentran ubicados fuera del territorio del Espacio Económico Europeo. Será necesario obtener la autorización del Director de la Agencia Española de Protección de Datos, salvo que se trate de alguno de los supuestos excepcionados por la normativa aplicable.

Normativa aplicable: art. 20.2.e), 33 y 34 LOPD; 54.1.e), 65 y ss. 137 y ss. RLOPD.

5.5 Los derechos de *habeas data* o derechos ARCO

Las personas titulares de los datos, como parte de su derecho a la autodeterminación informativa, disponen de los derechos de acceso, rectificación, cancelación y oposición. Estos derechos, conocidos como derechos de habeas data o con el acrónimo "derechos ARCO", se caracterizan por ser:

a) **Personalísimos:** sólo los puede ejercer la persona titular de los datos, salvo los supuestos siguientes:

- Cuándo la persona afectada está en situación de incapacidad o minoría de edad, que le imposibilita ejercer personalmente estos derechos, los puede ejercitar su representante legal, que tiene que acreditar esta condición.
- Cuando se actúa mediante un representante voluntario:

  Si se trata de ficheros de titularidad privada, hay que aportar copia del DNI o equivalente y de la representación conferida. La utilización de firma electrónica identificativa de la persona afectada exime de la presentación de las fotocopias del DNI o documento equivalente.

  Si se trata de ficheros de titularidad pública, la representación se tiene que acreditar por cualquier medio válido en derecho que deje constancia fidedigna o mediante la comparecencia personal de la persona afectada.

b) **Independientes:** en ningún caso el ejercicio de uno de estos derechos constituye un requisito previo para ejercer otro.

c) **Gratuitos:** estos derechos se tienen que poder ejercer por un medio sencillo que no suponga un ingreso adicional para el responsable del tratamiento. No se considera adecuado exigir el envío de cartas certificadas o semblantes, utilizar servicios de telecomunicaciones que impliquen una tarifación adicional al afectado o cualesquiera otro medio que implique un coste excesivo para el interesado.

Los centros educativos tienen que adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento que tiene que seguir el afectado para ejercer sus derechos.

Estos derechos se pueden ejercer a través de los servicios de atención al público, de información o de reclamaciones que tengan los centros, si así lo han previsto.

◊ ¿Un menor puede ejercer los derechos ARCO?

El menor mayor de 14 años puede ejercer los derechos de acceso, rectificación, cancelación y oposición sin necesidad de la autorización de sus padres o tutor, a menos que la normativa específica aplicable exija la asistencia de los padres o tutor.

El menor de 14 años tiene que ejercer los derechos ARCO a través de la representación de sus padres o tutor.

5.5.1 Derecho de acceso

Mediante este derecho, la persona afectada tiene derecho a conocer:

- Sus datos de carácter personal que son objeto de tratamiento.
- La finalidad del tratamiento.
- El origen de estos datos.
- Las comunicaciones que se han hecho o que se han previsto hacer.

¿Quién lo puede ejercer?

La persona afectada o un representante en nombre suyo (en el caso de menores de 14 años, personas discapacitadas, personas mayores de 14 años si la ley lo exige, o cuando la persona afectada designe voluntariamente a alguien que la represente).

¿Cómo se solicita?

Con un escrito dirigido al responsable del fichero, con el contenido siguiente:

- Nombre y apellidos de la persona que ejerce el derecho y del representante, si es el caso.
- Fotocopia del documento que acredita la identidad de la persona afectada y la identidad del representante, si lo hay (DNI, pasaporte o documento equivalente) o instrumentos electrónicos análogos (por ejemplo, certificado digital).
- Documento o instrumento electrónico acreditativo de la representación, si es el caso.
- Petición concreta: hay que indicar de forma clara y detallada lo que se pide.
- Dirección, fecha y firma de la persona que ejerce el derecho o de su representante.

El derecho se puede ejercer en relación con datos concretos, con los datos incluidos en un determinado fichero o con la totalidad de los datos tratados.

En casos de complejidad especial, el responsable del fichero puede facilitar a la persona afectada una lista de sus ficheros y pedirle que especifique respecto de cuáles pretende ejercer su derecho.

¿Cómo se ha de hacer efectivo?

El responsable del fichero, incluso si no dispone de datos de la persona afectada, tiene que notificarle la respuesta en el plazo de un mes a partir de la recepción de la solicitud. Si la resolución es estimatoria y no se acompaña la información solicitada, hay que hacer efectivo el acceso en el plazo de 10 días hábiles, de acuerdo con el sistema designado por la persona afectada.

La persona afectada puede pedir que el derecho de acceso se haga efectivo a través de los **sistemas de consulta** siguientes:

- Visualización en pantalla.
- Escrito, copia o fotocopia, por correo certificado u ordinario.
- Correo electrónico u otros sistemas de comunicación electrónica.
- Cualquier otro sistema que sea adecuado a las características del fichero.

Si el centro ofrece un determinado sistema para hacer efectivo el derecho de acceso y la persona afectada lo rechaza, el centro no tiene que responder de los riesgos para la seguridad de la información que se pueden derivar de la elección.

Si la persona afectada exige que el derecho de acceso se materialice mediante un procedimiento que implica un coste desproporcionado respecto del ofrecido por el responsable, con los mismos efectos y garantizando la misma seguridad, los gastos derivados de su elección son a su cargo.

¿Cuándo no se tiene que dar el acceso?

Motivos de denegación o limitación del derecho de acceso:

- Si hay una prohibición legal.
- Si ya se ha ejercido el mismo derecho en los doce meses anteriores a la solicitud, a menos que la persona interesada acredite un interés legítimo que lo justifique.

- En ficheros policiales:
  - Si hay peligro para la defensa del Estado.
  - Por cuestiones de seguridad pública.
  - Para proteger los derechos y las libertades de terceros.
  - Por necesidades de una investigación policial.
- En ficheros de la hacienda pública:
  - Cuando puede obstaculizar las actuaciones administrativas encaminadas a asegurar el cumplimiento de las obligaciones tributarias.
  - Cuando la persona afectada está siendo objeto de actuaciones inspectoras.

◊ ¿Cómo puede un alumno conocer la información que tiene un centro educativo sobre su persona?

Ejerciendo el derecho de acceso previsto a la LOPD mediante solicitud dirigida al centro, acompañada de una copia del DNI e indicando el fichero o ficheros a consultar.

En caso de que sea menor de 14 años, la solicitud la tienen que formular sus padres o tutor.

◊ ¿A qué datos se puede acceder en virtud de este derecho?

El acceso, tiene que limitarse a sus propios datos. En caso contrario se produciría una cesión o comunicación no amparada por la LOPD. El acceso incluye:

- Los datos personales concretos que son objeto de tratamiento.
- La finalidad del tratamiento.
- El origen de estos datos.
- Las comunicaciones que se han hecho o que se han previsto hacer.

◊ ¿Los padres pueden pedir el acceso a la documentación de su hijo menor de 14 años que conste en un centro educativo?

Sí, vista la condición de representante legal del menor.

◊¿Los padres pueden pedir la información relativa a las ausencias o retrasos y sus justificaciones?

Sí. Forma parte de la información relativa al menor. Ahora bien, sin perjuicio de la obligación de responder en todos los casos la solicitud, la obligación de comunicarla está condicionada a que el centro haya recogido estos datos y todavía las conserve.

◊¿Se puede dar acceso a cualquiera de los progenitores a los informes de evaluación pedagógica de los hijos, si los padres están separados?

Se puede dar acceso a cualquiera de los padres siempre que tengan atribuida la patria potestad del menor, con independencia de quien tenga la custodia.

Si uno de los progenitores está privado judicialmente de la patria potestad, para que pueda acceder a la información del menor, el centro educativo tiene que pedir el consentimiento del progenitor que tiene atribuida la patria potestad.

◊¿Se puede denegar el acceso a la información relativa a la preinscripción por el hecho de que no se dispone de los documentos originales de preinscripción?

No, el soporte en el cual se encuentre la información, o el hecho de que el documento no sea original, no justifica la denegación de este derecho.

◊¿Es posible denegar el ejercicio del derecho de acceso por la dificultad o el elevado coste que puede suponer para el centro?

No. La LOPD requiere al responsable del fichero que los datos de carácter personal se almacenen de forma que permitan ejercer el derecho de acceso, a menos que hayan sido legalmente canceladas. Aun así, se puede denegar si el interesado ejerció el mismo derecho en los 12 meses anteriores, a menos que se acredite un interés legítimo que lo justifique.

En el anexo 2 de esta Guía, se ofrece un modelo para ejercer el derecho de acceso.

Normativa aplicable: art. 15, 23 LOPD; 2.4 y 27 y ss. y 50 RLOPD; 15 Decreto 134/1999; 13 Instrucción 1/2009.

5.5.2 Derecho de rectificación

Mediante este derecho, la persona afectada puede pedir al centro educativo responsable del fichero que rectifique los datos inexactos o incompletos.

¿Quién lo puede ejercer?

La persona afectada o un representante en nombre suyo (en el caso de menores de 14 años, personas discapacitadas, personas mayores de 14 años si la ley lo exige, o cuando la persona afectada designe voluntariamente a alguien que la represente).

¿Cómo se solicita?

Con un escrito dirigido a la persona responsable del fichero, con el contenido siguiente:

- Nombre y apellidos de la persona que ejerce el derecho y del representante, si es el caso.
- Fotocopia del documento que acredita la identidad de la persona afectada y la identidad del representante, si lo hay (DNI, pasaporte o documento equivalente), o instrumentos electrónicos análogos (por ejemplo, certificado digital).
- Documento o instrumento electrónico acreditativo de la representación, si es el caso.

- Petición concreta: hay que indicar de forma clara y detallada lo que se pregunta, a qué datos se refiere y qué corrección se tiene que hacer.
- Dirección, fecha y firma de la persona que ejerce el derecho o de su representante.

La solicitud tiene que ir acompañada de la documentación que justifica la rectificación, si procede.

¿Cómo se ha de hacer efectivo?

- El responsable tiene que notificar la resolución sobre la solicitud de rectificación en el plazo de 10 días hábiles desde su recepción.
- Si los datos rectificados se han cedido previamente, el responsable del fichero tiene que notificar las rectificaciones al destinatario en un plazo de 10 días hábiles desde la resolución, para que las rectifique, también, en un plazo de 10 días.

¿En qué supuestos se puede denegar?

El derecho de rectificación se puede denegar en los supuestos siguientes:

- Cuando una ley o norma de derecho comunitario aplicable lo impide.
- Si hay una ley o una norma de derecho comunitario de aplicación directa que impide revelar la existencia del tratamiento.
- En ficheros policiales:
  – Si hay peligro para la defensa del Estado.
  – Por cuestiones de seguridad pública.
  – Para proteger los derechos y las libertades de terceros.
  – Por necesidades de una investigación policial.

- En ficheros de la hacienda pública:
  - Cuando puede obstaculizar las actuaciones administrativas encaminadas a asegurar el cumplimiento de las obligaciones tributarias.
  - Cuando la persona afectada está siendo objeto de actuaciones inspectoras.

◊¿Los alumnos pueden pedir la rectificación de los datos erróneos o inexactos que el centro educativo tiene en sus ficheros?

Sí. Los alumnos mayores de 14 años, o sus padres o tutor si es menor de esta edad, pueden pedirlo indicando los datos erróneos o inexactos que se tienen que corregir y aportando la documentación que lo acredita.

Normativa aplicable: art. 16, 23 LOPD; 31 y ss. y 50 RLOPD; 14 Instrucción 1/2009.

5.5.3 Derecho de cancelación

Mediante este derecho, la persona afectada puede pedir al centro educativo responsable del fichero que suprima los datos inadecuados o excesivos.

La cancelación de los datos no equivale al borrado o la destrucción física. La cancelación da lugar al "bloqueo", entendido como la identificación y reserva de estos datos con la finalidad de impedir su tratamiento, excepto para ponerlos a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de las responsabilidades mencionadas. Una vez transcurrido el plazo de prescripción de posibles responsabilidades, sí que hay que suprimir los datos, es decir, eliminarlos.

¿Quién lo puede ejercer?

La persona afectada o un representante en nombre suyo (en el caso de menores de 14 años, personas discapacitadas, personas más mayores de 14 años si la ley lo exige, o cuando la persona afectada designe voluntariamente a alguien que la represente).

¿Cómo se solicita?

Con un escrito dirigido al responsable del fichero con el contenido siguiente:

- Nombre y apellidos de la persona que ejerce el derecho y del representante, si es el caso.
- Fotocopia del documento que acredita la identidad de la persona afectada y la identidad del representante, si lo hay (DNI, pasaporte o documento equivalente), o instrumentos electrónicos análogos (por ejemplo, certificado digital).
- Documento o instrumento electrónico acreditativo de la representación, si es el caso.
- Petición concreta: hay que indicar de forma clara y detallada lo que se pide, y a qué datos se refiere.
- Dirección, fecha y firma de la persona que ejerce el derecho o de su representante.

Hay que adjuntar documentos que acreditan o justifican la cancelación, si procede.

¿Cómo se ha de hacer efectivo?

- El centro tiene que notificar la resolución sobre la solicitud de cancelación, en el plazo de 10 días hábiles desde su recepción.

- Si los datos rectificados se han cedido previamente, el responsable del fichero tiene que notificar las rectificaciones al destinatario en un plazo de 10 días hábiles desde la resolución, para que las cancele, también, en un plazo de 10 días.

¿Cuándo no se pueden cancelar los datos?

No se pueden cancelar los datos:

- Cuando se tienen que conservar durante los plazos previstos a las disposiciones aplicables.
- Cuando se tienen que conservar en el marco de relaciones contractuales entre el interesado y el responsable del fichero.
- Cuando una ley o norma de derecho comunitario aplicable lo impide.
- Cuando una ley o norma de derecho comunitario de aplicación directa impide al responsable revelar la existencia del tratamiento de los datos a que se refiere la cancelación.
- En ficheros policiales:
  – Si hay peligro para la defensa del Estado.
  – Por cuestiones de seguridad pública.
  – Para proteger los derechos y las libertades de terceros.
  – Por necesidades de una investigación policial.
- En ficheros de la hacienda pública:
  – Cuando puede obstaculizar las actuaciones administrativas encaminadas a asegurar el cumplimiento de las obligaciones tributarias.
  – Cuando la persona afectada está siendo objeto de actuaciones inspectoras.

◊¿Un centro educativo está obligado a cancelar los datos bancarios que había facilitado el alumno o su tutor para pagar las cuotas, si el alumno o sus representantes lo solicitan?

Sí, a menos que sea imprescindible mantenerlas para cobrar las cuotas derivadas de la relación jurídica establecida entre el centro y el alumno.

◊¿Puede un padre o madre separado ejercer el derecho de cancelación en nombre del alumno? ¿Hay que contar con el consentimiento del otro progenitor?

Cualquiera de ambos progenitores puede ejercer el derecho de cancelación sin contar con el consentimiento del otro, siempre que ambos tengan atribuida la patria potestad.

◊¿Un centro educativo puede cancelar toda la información contenida en el expediente académico de un exalumno, si éste lo solicita?

No. Con respecto a la conservación de la información contenida en los expedientes académicos, la documentación que generan los centros educativos, específicamente la referida al ejercicio de la función educativa, tiene valor documental. Por lo tanto hay que tener en cuenta la normativa de archivos (Ley 10/2001).

Para determinar qué información de los expedientes académicos hay que conservar, cómo se tiene que conservar y cuál se puede cancelar, se tiene que tener en cuenta lo que establezca la administración pública educativa y, si procede, las tablas de evaluación documental que se elaboren de acuerdo con la normativa de archivos.

Normativa aplicable: art. 16 LOPD; art. 9 Ley 10/2001; 2.4, 5.1.b), 8.6, 31 y ss. y 50 RLOPD; 15 Instrucción 1/2009.

5.5.4 Derecho de oposición

El ejercicio de este derecho impide al responsable del fichero, en este caso el centro, tratar los datos personales de las personas afectadas. Si el tratamiento ya se ha iniciado, obliga a dejar de tratarlos, en los supuestos siguientes:

- Cuando, en tratamientos para los cuales no sea necesario el consentimiento de la persona afectada, y siempre que una ley no disponga el contrario, hay un motivo legítimo y fundamentado referido a su situación personal concreta que lo justifica.
- Cuando se trata de ficheros destinados a actividades publicitarias y de prospección comercial.
- Cuando el tratamiento tiene como finalidad adoptar una decisión con efectos jurídicos referida a la persona afectada, basada únicamente en un tratamiento automatizado.

¿Quién lo puede ejercer?

La persona afectada o un representante en nombre suyo (en el caso de menores de 14 años, personas discapacitadas, personas mayores de 14 años si la ley lo exige, o cuando la persona afectada designa voluntariamente a alguien que la represente).

¿Cómo se solicita?

Con un escrito dirigido al responsable del fichero, con el contenido siguiente:

- Nombre y apellidos de la persona que ejerce el derecho y del representante, si es el caso.
- Fotocopia del documento que acredita la identidad de la persona afectada y la identidad del representante, si lo hay (DNI, pasaporte o documento equivalente), o instrumentos electrónicos análogos (por ejemplo, certificado digital).

- Documento o instrumento electrónico acreditativo de la representación, si es el caso.
- Petición concreta: hay que indicar de forma clara y detallada lo que se pide.
- Se tienen que hacer constar los motivos fundamentados y legítimos.
- Dirección, fecha y firma de la persona que ejerce el derecho o de su representante.

Hay que adjuntar documentos que acrediten lo que se pide, si procede.

¿Cómo se ha de hacer efectivo?

El responsable del fichero tiene que notificar la resolución sobre la solicitud de oposición en el plazo de 10 días hábiles desde su recepción.

¿Cuándo se puede denegar el derecho de oposición?

El derecho de oposición se puede denegar en los supuestos siguientes:

- En caso de que la solicitud se base en un motivo referido a su situación personal concreta:
  – Cuando no se alega un motivo legítimo y fundamentado relativo a una situación personal que justifica el cese del tratamiento.
  – Cuando una disposición legal no lo permite.
- En el caso de decisiones que evalúen aspectos de la personalidad basadas únicamente en un tratamiento automatizado de datos:
  – Cuando la decisión se ha adoptado dentro del contexto de la celebración o la ejecución del contrato a petición del interesado, se le ha informado de que se adoptarán este tipo de decisiones y se le ha dado la posibilidad de defender su derecho o interés.
  – Cuando la evaluación de la personalidad está autorizada por ley.

◊¿Un alumno se puede oponer a la publicación de su admisión en un centro educativo?

El alumno se puede oponer a este tratamiento, de conformidad con el artículo 6.4 de la LOPD, si alega motivos fundamentados y legítimos relativos a su situación personal concreta, como por ejemplo por razones de seguridad por ser víctima de violencia de género o sufrir algún tipo de amenaza, etc. En este caso, el centro lo tiene que excluir del listado de admitidos que se publique. Si es menor de 14 años, el derecho lo tienen que ejercer sus padres o tutor.

Normativa aplicable: art. 6.4 LOPD; 34 y ss., 51 RLOPD; 16 Instrucción 1/2009.

5.5.5 Aspectos comunes del procedimiento para ejercer los derechos ARCO

¿Dónde se tiene que presentar la solicitud?

El afectado tiene que presentar la solicitud en el centro que trata sus datos o, si procede, al encargado del tratamiento. El acuerdo de creación del fichero tiene que indicar el lugar donde se pueden ejercer los derechos.

Cuando el centro dispone de un servicio de atención al público o de ejercicio de reclamaciones, conviene que al establecerse el lugar donde se pueden ejercer los derechos ARCO se prevea que la persona afectada se pueda dirigir para ejercerlos.

Los derechos también se pueden ejercer delante del encargado del tratamiento. En este caso, el encargado (por ejemplo, la empresa que presta el servicio de comedor) tiene que trasladar la solicitud al centro para que la resuelva, salvo los casos en que el contrato de encargo del tratamiento lo habilite para resolver las solicitudes por cuenta del colegio.

¿A través de qué medio?

Se pueden ejercer a través de un medio que permita acreditar la presentación de la solicitud. El responsable del fichero o tratamiento tiene que atender la solicitud aunque el interesado no haya utilizado el procedimiento establecido específicamente a este efecto, siempre que se haya utilizado un medio que permita acreditar el envío y la recepción.

Si la solicitud no reúne los requisitos establecidos por el artículo 25.1 RLOPD, el centro tiene que pedir la subsanación.

Sobre el contenido de la solicitud, se puede consultar a los modelos para ejercer los derechos ARCO (anexos 2 a 5).

¿Hay que resolver siempre la solicitud?

El responsable del fichero siempre tiene que responder la solicitud dentro del plazo establecido para atender cada uno de los derechos.

Una vez transcurrido el plazo establecido para la resolución, la solicitud se tiene que entender desestimada.

¿Y si se ha denegado el derecho?

En caso de que se deniegue el ejercicio del derecho al interesado, la decisión se tiene que motivar y hay que informar a la persona afectada sobre su derecho a reclamar la tutela ante la Autoridad Catalana de Protección de Datos.

◊¿El responsable del fichero puede excluir la posibilidad de ejercer los derechos ARCO a través del correo electrónico?

No. El interesado puede utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud, en los términos del artículo 25.1 RLOPD.

◊¿Se tiene que responder la solicitud, cuando no están los datos en el fichero o ya se han cancelado?

Sí. Con independencia de si los datos se conservan o se han cancelado, las solicitudes de ejercicio de los derechos siempre se tienen que responder de forma expresa y dentro del plazo establecido, incluso en caso de que nunca se haya dispuesto de datos de la persona solicitante.

◊¿El responsable del fichero puede dejar de atender una solicitud por falta de algunos de los requisitos formales?

No, en caso de que falten algunos de los requisitos formales, el responsable del fichero tiene que solicitar la subsanación, dentro del plazo para responderla y con la máxima celeridad posible.

Normativa aplicable: art. 17 LOPD; 6, 25, 29.3, 32.3, 35.3, 44, 50, 117 y ss. RLOPD; 17 Instrucción 1/2009.

5.5.6 Reclamación de tutela de derechos

La tutela de derechos se ejerce mediante un procedimiento que se tramita ante la Autoridad Catalana de Protección de Datos y que se inicia a instancia de la persona afectada:

- Para ejercer sus derechos, el ciudadano se tiene que dirigir al responsable del fichero. En caso de que esta solicitud no se responda dentro del plazo legalmente establecido o se deniegue el ejercicio, se puede dirigir a la Autoridad Catalana de Protección de Datos mediante una reclamación de tutela de derechos.

- La Autoridad traslada la reclamación al responsable del fichero y, una vez recibidas las alegaciones dentro del plazo legalmente establecido y practicadas todas las pruebas, tiene que resolver sobre la reclamación y notificarla, en el plazo de 6 meses desde la fecha de entrada de la reclamación. Si no se resuelve dentro de este plazo, la reclamación de tutela se considera desestimada.
- Cuando la resolución de la reclamación sea estimatoria, se tiene que requerir el responsable del fichero para que en el plazo de los 10 días hábiles siguientes a la notificación, haga efectivo el derecho reclamado.

Normativa aplicable: art. 18 LOPD; 5. b) y 16 LACPD; 117 y ss. RLOPD.

5.6 Medidas de seguridad

5.6.1 Implementación de las medidas de seguridad

Los responsables y los encargados del tratamiento tienen que implementar una serie de medidas de seguridad, de índole técnica y organizativa, adecuadas a las diferentes tipologías de datos que se tratan, con la finalidad de evitar la alteración, la pérdida o que terceros no autorizados accedan o los traten.

De acuerdo con la normativa en materia de protección de datos, el **responsable** del fichero y, si procede el encargado del tratamiento tienen que adoptar las medidas necesarias en cada caso, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados, el sistema de tratamiento utilizado (automatizado o no) y los riesgos a los cuales están expuestos, ya sean provenientes de la acción humana o del medio físico o natural.

Por otra parte, la LOE establece que en el tratamiento de los datos del alumnado se tienen que aplicar normas técnicas y organizativas que garanticen su seguridad y confidencialidad.

Cuando hay un **encargado del tratamiento**, le son de aplicación las mismas obligaciones relativas a las medidas de seguridad que al responsable del fichero, de acuerdo con lo que dispone el contrato de encargo del tratamiento.

El RLOPD establece las medidas necesarias de acuerdo con el tipo de datos tratados y el soporte en el cual estén almacenados. Las medidas de seguridad se determinan a partir de **tres niveles de seguridad**.

Los niveles de seguridad se determinan atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad, la integridad y la disponibilidad de la información:

- **Nivel básico:** aplicable a todos los ficheros o tratamientos de datos personales.
- **Nivel medio:** se aplica a los ficheros o tratamientos que contienen datos relativos a:
  a) La comisión de infracciones administrativas o penales.
  b) Información sobre la solvencia patrimonial y crédito que traten entidades que prestan estos servicios.
  c) El ejercicio de potestades tributarias por parte de administraciones tributarias.
  d) La prestación de servicios financieros por entidades financieras.
  e) El ejercicio de competencias de las entidades gestoras de la seguridad social y mutuas de accidentes de trabajo y enfermedades profesionales.
  f) La evaluación de la personalidad o el comportamiento de los individuos.

Los ficheros de los operadores de servicios de comunicaciones electrónicas disponibles al público o redes públicas de comunicaciones electrónicas, que contienen datos relativos al tráfico y la localización, tienen que adoptar medidas de nivel medio además de la implantación de un registro de accesos.

- **Nivel alto:** se aplica a los ficheros o tratamientos que contienen datos relativos a:

  a) Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

  b) Recogidos para finalidades policiales, sin el consentimiento de las personas afectadas.

  c) Actos de violencia de género.

  No obstante, es suficiente aplicar el nivel básico o medio, según procede:

  – Cuando los datos se utilizan con la única finalidad de hacer una transferencia dineraria a las entidades de que los afectados sean asociados o miembros.

  – Cuando se incluyen estos datos de forma incidental o accesoria, sin tener relación con su finalidad.

  – Cuando los datos de salud se refieren exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

A **título orientativo**, el nivel de seguridad que se podría asignar en los ficheros más habituales de un centro educativo podría ser el siguiente:

Ficheros	Nivel de seguridad
Recursos humanos	Medio
Alumnos	Alto
Proveedores	Básico
Contabilidad	Básico
Contactos	Básico
Videovigilancia	Básico

En cualquier caso, se trata sólo de indicaciones orientativas. La determinación exacta del nivel de seguridad aplicable dependerá de la configuración de cada fichero concreto. Así, por ejemplo, puede ser necesario implantar medidas de seguridad de

nivel alto en el fichero de recursos humanos, si se recogen datos de salud diferentes al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

Una vez determinado el nivel de seguridad que corresponde atribuir a cada fichero, y según el sistema de tratamiento que se utiliza, el RLOPD establece las medidas de seguridad que corresponden a cada uno. Los niveles son acumulativos, de manera que cada nivel, además de las medidas específicas que tiene previstas, tiene que aplicar también las medidas del nivel o niveles anteriores.

Ficheros y tratamientos automatizados			
Medidas	**Nivel básico**	**Nivel medio**	**Nivel alto**
Funciones y obligaciones del personal	Art. 89	Art. 89	Art. 89
Registro de incidencias	Art. 90	Art. 100	Art. 100
Control de acceso	Art. 91	Art. 91	Art. 91
Gestión de soportes y documentos	Art. 92	Art. 97	Art. 101
Identificación y autentificación	Art. 93	Art. 98	Art. 98
Copias de seguridad y recuperación	Art. 94	Art. 94	Art. 102
Responsable de seguridad		Art. 95	Art. 95
Auditoría		Art. 96	Art. 96
Control de acceso físico		Art. 99	Art. 99
Registro de accesos			Art. 103
Telecomunicaciones			Art. 104

Ficheros y tratamientos no automatizados			
Medidas	**Nivel básico**	**Nivel medio**	**Nivel alto**
Funciones y obligaciones del personal	Art. 105.2 y 89	Art. 105.2 y 89	Art. 105.2 y 89
Registro de incidencias	Art. 105.2 y 90	Art. 105.2 y 90	Art. 105.2 y 90
Control de acceso	Art. 105.2 y 91	Art. 105.2 y 91	Art. 105.2 y 91
Gestión de soportes y documentos	Art. 105.2 y 92	Art. 105.2 y 92	Art. 105.2 y 92
Criterios de archivo	Art. 106	Art. 106	Art. 106
Dispositivos de almacenamiento	Art. 107	Art. 107	Art. 107
Custodia de los soportes	Art. 108	Art. 108	Art. 108
Responsable de seguridad		Art. 109	Art. 109
Auditoría		Art. 110	Art. 110
Almacenaje de la información			Art. 111
Copia o reproducción			Art. 112
Acceso a la documentación			Art. 113
Traslado de documentación			Art. 114

Las medidas previstas en el RLOPD tienen el carácter de mínimos, por lo cual el responsable del fichero puede aplicar unas medidas de seguridad superiores si lo considera conveniente. Aparte de estas medidas de seguridad concretas, son aplicables a todos los tratamientos las garantías previstas en el RLOPD respecto de:

- Prestación de servicios por un encargado del tratamiento (art. 82)
- Prestación de servicios sin acceso a datos personales (art. 83)
- Delegación de autorizaciones (art. 84)
- Acceso a datos a través de redes de comunicaciones (art. 85)
- Régimen de trabajo fuera de los locales del responsable del fichero o del encargado del tratamiento (art. 86)

- Ficheros temporales o copias de trabajo (art. 87)
- Documento de seguridad (art. 88)

Conviene destacar la importancia de adoptar las medidas de seguridad necesarias para asegurar la integridad de la información, especialmente en las informaciones publicadas en el web del centro. A estos efectos, conviene implantar un sistema robusto de identificación de los administradores y editores, para evitar que personas no autorizadas manipulen el contenido del web.

◊¿Qué nivel de medidas de seguridad tiene que tener el fichero de alumnos del centro educativo?

Depende de los datos personales que contenga. Probablemente, requerirá nivel alto dado que es previsible que contenga información sobre el estado de salud física o psíquica de los alumnos o, como mínimo, respecto de algunos de ellos.

Cuando la información esté en un soporte no automatizado, los armarios, archivadores u otros elementos en que se conserve la documentación se tienen que ubicar en dependencias cerradas a las cuales sólo puedan acceder directamente las personas autorizadas.

◊¿Qué nivel de seguridad tiene que tener el fichero donde se recogen los datos de los alumnos que utilizan el servicio de comedor?

Dado que previsiblemente se pueden recoger datos sobre alumnos que tienen que seguir dietas específicas que se pueden asociar a determinadas enfermedades o religiones, hay que aplicar medidas de nivel alto.

◊¿Cuáles son los requisitos mínimos de seguridad que debe ofrecer una plataforma de gestión académica o administrativa de un centro educativo?

Sin perjuicio de la adopción de las adecuadas medidas de seguridad previstas en el RLOPD, cualquier plataforma o software de gestión del centro educativo debe garantizar:

- Conexión segura HTTPS en todas las secciones del sistema cuando el acceso se realice mediante redes públicas de telecomunicaciones.
- Gestión de incidencias de seguridad.
- Autentificación de usuarios, con permisos específicos para cada perfil de usuario (administradores del centro, padres, alumnos y maestros).
- Historial de acceso de los usuarios del sistema.
- Mecanismos para prevenir la fuga de datos y evitar su exportación masiva.
- Gestión de soportes y documentos, como mínimo en lo que se refiere a su identificación.
- Copias de seguridad periódicas de todos los datos, que incluya sistemas para verificar su calidad.
- Seguridad lógica: ausencia de virus y de otras amenazas externas.
- Seguridad física y del entorno, especialmente en relación con los equipos que hagan las funciones de servidor de datos y aplicaciones.

◊¿Qué nivel de medidas de seguridad se tiene que aplicar al campus virtual o entorno virtual de aprendizaje de un centro educativo?

Depende del contenido del campus virtual o del entorno virtual de aprendizaje. Normalmente requerirá nivel medio dado que puede permitir la obtención de perfiles (actas de evaluación, calificaciones, observaciones académicas, servicio de correo electrónico y mensajería, etc.), a no ser que se incorporen también datos especialmente protegidos (por ejemplo, certificados médicos acreditativos de enfermedades), en qué hay que aplicar un nivel alto.

En cualquier caso, conviene destacar especialmente la implantación de un sistema de identificación y autenticación de los usuarios que sea robusto.

◊¿Cualquier trabajador de un centro educativo puede acceder a toda la información sobre terceras personas de que dispone el centro?

Los trabajadores sólo pueden tener acceso a la información necesaria para ejercer las funciones que tienen atribuidas.

◊¿Los maestros pueden llevarse información personal de los alumnos a casa (fichas de los alumnos, informes de seguimiento, etc.)?

La normativa de protección de datos establece que, con carácter general, la salida de soportes y documentos que contienen datos personales fuera de los locales del responsable la tiene que autorizar el mismo responsable o estar autorizada en el documento de seguridad.

En cualquier caso, la autorización implica necesariamente que los maestros deben conocer las medidas de seguridad que es necesario aplicar durante el traslado de la documentación y durante la custodia de la información a su casa. Es necesario evitar que los documentos se pierdan o que terceras personas no autorizadas accedan a la información. El mantenimiento de los datos fuera del centro sólo debe prolongarse el tiempo mínimo imprescindible.

◊¿Y si el acceso a dicha información personal se produce a través de una aplicación instalada en el Smartphone o la tableta del maestro?

Si el centro educativo lo autoriza, los maestros podrán acceder, des de fuera del centro educativo, a los datos de los alumnos a través de sus dispositivos móviles.

En estos casos es importante cumplir la política de seguridad del centro educativo relativa al uso de usuarios y contraseñas, evitar el uso de redes WI-FI que no ofrezcan confianza, no almacenar información sensible en local en estos dispositivos, así como, en caso de robo o pérdida del dispositivo, avisar inmediatamente al responsable de seguridad o a la persona que corresponda.

Resultarían aplicables a estos supuestos las recomendaciones hechas en la cuestión anterior en relación con la necesidad de conocer las normas de seguridad y evitar el acceso de terceros no autorizados. Dichos consejos también deben tenerse en cuenta cuando el acceso se produzca desde dentro del centro utilizando este tipo de dispositivos móviles.

◊¿Qué nivel de seguridad se tiene que aplicar a los ficheros de recursos humanos donde aparecen datos relativos a la afiliación sindical, cuando se recojan exclusivamente para hacer una transferencia de las cuotas sindicales al sindicato correspondiente?

De acuerdo con el arte. 81.5.a) RLOPD, no es exigible aplicar medidas de nivel alto a los datos que, a pesar de tener asignado en principio este nivel, se utilizan con la única finalidad de hacer una transferencia dineraria a las entidades de los cuales los afectados sean asociados o miembros. Por lo tanto, se les tiene que aplicar el nivel básico o medio, dependiendo del resto de datos que contenga el fichero.

◊¿Qué nivel de seguridad requieren los ficheros que contienen datos relativos a la condición de discapacidad o invalidez de la persona afectada o al grado de la discapacidad?

Se les tiene que aplicar el nivel alto, dado que es un dato de salud. No obstante, se les puede aplicar el nivel básico o medio, dependiendo del resto de datos que contenga el fichero, siempre que el dato tratado sea exclusivamente el relativo a la concurrencia de una discapacidad o a su grado y se trate para el cumplimiento de un deber público (art. 81.6 RLOPD).

◊¿La utilización de servicios de "cloud storage" conlleva riesgos para la seguridad de los datos personales que el centro educativo decide almacenar?

Sí. Debe tenerse en cuenta que el funcionamiento propio de estos servicios, así como las diferentes aplicaciones y plataformas que permiten el acceso y la gestión de los archivos almacenados, pueden presentar vulnerabilidades que afecten la información almacenada, especialmente en relación con su confidencialidad, debido a accesos no autorizados.

Además, deben tenerse en cuenta los riesgos inherentes al mecanismo de acceso utilizado para acceder a estos servicios, ya sea mediante el navegador o las aplicaciones instaladas en smartphones u ordenadores personales.

◊¿Qué precauciones puede adoptar el centro educativo en la utilización de servicios de “cloud storage”?

• Sin perjuicio del cumplimiento de las adecuadas medidas de seguridad, se recomienda:

- Escoger aquellos servicios de “cloud storage” que proporcionen un sistema de cifrado de la información antes de su almacenamiento en la nube. De no proporcionarlo, usar aplicaciones externas para cifrar la información con anterioridad a su almacenamiento.
- Examinar minuciosamente qué información se quiere almacenar, así como qué parte de dicha información puede ser compartida.
- Utilizar contraseñas seguras para las cuentas de usuario (combinar números, letras, símbolos, mayúsculas y minúsculas, y establecer una longitud mínima de 8 caracteres).
- Utilizar la verificación en dos pasos cuando sea posible.
- Revisar la configuración por defecto del nivel de privacidad del servicio en lo que se refiere a la compartición de ficheros entre usuarios, para evitar publicar, sin conocimiento, información sin estar protegida per algún sistema de control de acceso.
- En el caso de transmitir enlaces para compartir documentos, sólo deben permitir el acceso a las personas previamente autorizadas. Siempre que el servicio lo permita, debe limitarse el tiempo que dicho enlace estará disponible.
- Hacer copias de seguridad periódicas de la información almacenada y, si es posible, mantener una copia sincronizada local en los ordenadores del centro.
- En el caso de usar acceso web al servicio, no escoger por la opción de recordar las credenciales, y cerrar la sesión al abandonar el puesto de trabajo.
- En el caso de usar la aplicación de escritorio para acceder al servicio, proteger el acceso al ordenador mediante un usuario (local o de red) y una contraseña, o con un mecanismo similar, y cifrar los documentos antes de enviarlos a los servicios de almacenamiento.
- En el caso de usar las aplicaciones de acceso de dispositivos móviles, proteger siempre el acceso al dispositivo y, si lo permite la aplicación, proteger también el acceso a la APP concreta.

- Controlar, en todo momento, qué dispositivos se encuentran vinculados a la cuenta del servicio (es decir, con qué dispositivos se sincroniza la información almacenada) y verificar periódicamente si es necesario desvincular alguno de ellos.

Normativa aplicable: art. 9,12 y 20.2.h) LOPD; ap. 3 DA 23ª LOE; D.A. 14ª LE; 54.1.h), 79 y ss. 89 y ss. 105 y ss. RLOPD; 19, 20 y 21 Instrucción 1/2009; Recomendación 1/2008; CNS 28/2011.

5.6.2 El documento de seguridad

El centro educativo, como responsable del fichero o tratamiento, tiene que elaborar un documento de seguridad que recoja las medidas de índole técnica y organizativa que el responsable del fichero y/o el encargado del tratamiento, si procede tienen que implementar en los ficheros que contienen datos personales.

El cumplimiento de las medidas previstas en este documento es obligatorio para todo el personal que tiene acceso a datos personales y a las aplicaciones informáticas y sistemas de información donde se tratan.

El documento de seguridad **tiene que mantenerse actualizado** en todo momento y revisarse siempre que se producen cambios relevantes que pueden repercutir en el cumplimiento de las medidas de seguridad implementadas o, si procede, como consecuencia de los controles periódicos realizados.

El documento de seguridad tiene que tener el contenido mínimo siguiente:

a) Ámbito de aplicación del documento, con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RLOPD.

c) Funciones y obligaciones del personal, en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Procedimientos de ejecución de copias de seguridad y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Medidas que hay que adoptar para transportar soportes y documentos, así como para destruir los documentos y los soportes o, si procede, reutilizarlos.

Si el fichero o tratamiento tiene nivel de seguridad medio o alto, además del contenido mínimo, el documento de seguridad tiene que contener la identificación del responsable o responsables de seguridad y los controles periódicos necesarios para verificar el cumplimiento de lo que se dispone en el mismo documento.

Responsable de seguridad

Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Si el centro educativo encarga el tratamiento a un tercero y los datos se tratan exclusivamente en los sistemas del encargado, esta circunstancia se tiene que hacer constar en el documento.

Cuando el centro educativo actúe como encargado del tratamiento, su documento de seguridad tiene que identificar:

- Ficheros o tratamientos que afecta
- Referencia al contrato o el acuerdo de encargo
- Identificación del responsable
- Vigencia del encargo

En los anexos de esta Guía se puede consultar un modelo de documento de seguridad para centros educativos.

◊¿Quién tiene que ser el responsable de seguridad?

El responsable de seguridad puede ser cualquier persona que, nombrada por el responsable del fichero, en este caso el centro educativo, coordine la implantación de las medidas de seguridad exigibles y haga el control.

◊¿Es necesario presentar el documento de seguridad ante la Autoridad Catalana de Protección de Datos?

No. El documento de seguridad es de carácter interno. Ahora bien, tiene que estar disponible y actualizado por si la Autoridad lo requiere.

◊¿Hay que tener en cuenta la normativa de archivos?

Sí. Cuando se trata de ficheros de titularidad pública, el documento de seguridad tiene que recoger el criterio de archivo utilizado, con sujeción a los criterios contenidos en la normativa de archivos.

Normativa aplicable: art. 5.2.l), 88, 95 RLOPD; 22 Instrucción 1/2009.

6 Obligaciones una vez ha finalizado el tratamiento de los datos

Una vez ha finalizado el tratamiento, hay que velar por el destino de los datos

Conservación y cancelación de los datos

De acuerdo con el principio de calidad, los datos se tienen que cancelar cuando dejen de ser necesarios o pertinentes para la finalidad para la cual se recogieron.

Excepcionalmente, se pueden conservar durante un periodo superior, en los supuestos siguientes:

- Disociación de los datos: cuando se anonimizan los datos o se disocia la información que contienen.

> **Dato disociado**
>
> Dato que no permite la identificación de un afectado o interesado.

- Finalidades históricas, estadísticas o científicas: cuando el tratamiento de los datos atienda a valores históricos, estadísticos o científicos de acuerdo con la legislación específica, los datos se pueden conservar con la autorización de la Autoridad Catalana de Protección de Datos.

> **Finalidades históricas, estadísticas o científicas**
>
> Con el fin de determinar si concurren estas finalidades, hay que atenerse a la legislación aplicable en cada caso y, en particular, a lo que disponen la Ley 12/1989, de 9 de mayo, reguladora de la función estadística pública; la Ley 16/1985, de 25 junio, del patrimonio histórico español, y la Ley 13/1986, de 14 de abril, de fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como la normativa autonómica en estas materias.

Por otra parte, los datos cancelados se tienen que conservar bloqueados, a disposición de las administraciones públicas, jueces y tribunales, durante el transcurso del tiempo en que se puede exigir algún tipo de responsabilidad derivada de una

relación u obligación jurídica, de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por la persona afectada. Transcurrido este plazo, se tienen que suprimir.

> **Bloqueo**
>
> Identificación y reserva de los datos personales, con la finalidad de impedir el tratamiento excepto para ponerlos a disposición de las administraciones públicas, jueces y tribunales, para atender las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de las responsabilidades mencionadas.

Ahora bien, si los datos se han obtenido por medios fraudulentos, desleales o ilícitos, se tienen que destruir directamente.

Para determinar el periodo de conservación de los documentos hay que tener en cuenta las previsiones sobre evaluación documental contenidas en la normativa de archivos.

La Comisión Nacional de Acceso, Evaluación y Elección de Documentos ha aprobado en el ámbito de enseñanza las tablas de evaluación documental siguientes:

- Código 93 (Departamento de Enseñanza): solicitudes de becas (DOGC 2117): destrucción total a los 3 años, a menos que se haya interpuesto recurso.
- Código 133 (ayuntamientos): expedientes de admisión y matriculación de alumnos en los centros de enseñanza (DOGC 2279): destrucción total a los cinco años.

Por otra parte, no consta que se hayan aprobado tablas de evaluación documental referidas a los expedientes o historiales de alumnos referidos a niveles de la enseñanza obligatoria. A efectos ilustrativos, recordar que la tabla relativa a los expedientes académicos de estudiantes universitarios (código 412, DOGC 3431) prevé la conservación permanente de los documentos que forman dichos expedientes.

◊¿Si la información personal se anonimiza o disocia de forma irreversible se cumple con la obligación de cancelar los datos?

La anonimización o disociación de un dato, de manera que no se pueda identificar a su titular, cumple con esta obligación de cancelación.

◊¿Se tienen que cancelar los datos de un alumno cuando deja de estudiar en un centro educativo?

Está justificado conservar de forma permanente los datos relativos al expediente académico. Con respecto al resto de información, cuando el centro no la necesite se tiene que bloquear y, superados los plazos de prescripción de eventuales responsabilidades, se tiene que suprimir.

◊¿Hay que conservar los datos de las personas que han hecho la preinscripción en un centro educativo y que no han sido admitidas?

La Tabla de evaluación documental con Código 133 (DOGC 2279) establece que se pueden destruir en el plazo de cinco años.

◊¿Hay que conservar los datos del alumno recogidos en el trámite de petición de una beca?

La Tabla de evaluación documental con Código 93 (DOGC 2117), establece que se pueden destruir en el plazo de tres años, a menos que se haya interpuesto recurso. En este caso, se tienen que conservar hasta que la resolución sea firme.

◊¿El servicio médico del centro educativo puede conservar los datos de salud del menor recogidos por los servicios sanitarios del centro, una vez ha finalizado su periodo de escolarización en el centro?

No. El centro ya no tiene que seguir tratando estos datos. Por lo tanto, hay que poner esta información a disposición de los padres o tutor del alumno o, si procede, del mismo alumno. Caso que no la recuperen, la información se tiene que cancelar.

◊¿Qué hay que hacer con la documentación que ya no se tiene que conservar bloqueada?

En caso de que la documentación contenga datos personales, se tiene que destruir de manera que terceros no autorizados no puedan acceder, mediante destructoras u otros sistemas que eviten su acceso.

Se recomienda establecer un protocolo para rechazar de forma segura este tipo de documentación e informar al personal.

Si se contrata una empresa para que la destruya, hay que firmar un contrato de encargo del tratamiento.

Normativa aplicable: art. 3.f), 4.5 y 4.7 LOPD; art. 9 Ley 10/2001; art. 5.1.b), 5.1.e), 5.1.p), 8.6, 9.1 y 157-158 RLOPD; 8 Instrucción 1/2009; CNS 42/2013.

7 El régimen de responsabilidad

El incumplimiento de la normativa de protección de datos puede comportar la exigencia de responsabilidades al responsable del fichero y/o al encargado del tratamiento

La vulneración del derecho a la protección de datos genera responsabilidades que se pueden exigir mediante una reclamación por los daños y perjuicios sufridos. Cuando los hechos sean constitutivos de alguna de las infracciones tipificadas en la LOPD, se pueden denunciar ante la Autoridad Catalana de Protección de Datos. Cuando sean constitutivos de delito o falta, se pueden denunciar ante el orden jurisdiccional penal. Todo eso sin perjuicio de las responsabilidades que se puedan derivar de la vulneración de otros derechos, como los derechos al honor, a la intimidad y a la propia imagen, reconocidos en la Constitución Española.

7.1 Tipo de responsabilidades

Las responsabilidades derivadas de un tratamiento ilícito de los datos personales pueden ser de diferentes tipos:

Responsabilidad patrimonial

Las personas titulares de los datos personales tienen derecho a que se las indemnice cuando sufren algún **daño o alguna lesión en sus bienes o derechos**, a consecuencia de la vulneración de lo que dispone la normativa de protección de datos.

Cuando el perjuicio proviene de ficheros o tratamientos de titularidad pública, la responsabilidad patrimonial puede reclamarse en vía administrativa, de acuerdo con la legislación reguladora del régimen de responsabilidad patrimonial de las administraciones públicas. Cuando proviene de ficheros o tratamientos de titularidad privada, puede reclamarse ante la jurisdicción ordinaria.

Responsabilidad administrativa

Los responsables de los ficheros y los encargados del tratamiento, tanto de titularidad pública como privada, están sujetos al régimen sancionador de la LOPD. La Autoridad Catalana de Protección de Datos aplica este régimen sancionador, en relación con ficheros de titularidad pública y privada, con respecto a las entidades incluidas dentro de su ámbito competencial.

Responsabilidad penal

El Código Penal tipifica el descubrimiento y la revelación de secretos como delito contra la intimidad. Se tipifican, entre otros, el apoderamiento, la utilización o la modificación, así como la difusión o cesión, sin consentimiento y en perjuicio de terceras personas, de datos reservados de carácter personal o familiar, que se encuentren en ficheros o soportes informáticos, electrónicos o telemáticos, o en archivos o registros, tanto públicos como privados.

◊¿Los interesados pueden reclamar una indemnización por los daños sufridos como consecuencia del incumplimiento de la normativa de protección de datos?

Si se trata de un fichero de titularidad pública, de acuerdo con la legislación reguladora del régimen de responsabilidad patrimonial de las administraciones públicas, pueden ejercer una acción de reclamación de responsabilidad ante el ente responsable y, si procede, ante la jurisdicción contenciosa administrativa.

Si la vulneración es relativa a un fichero de titularidad privada, se tiene que presentar demanda ante la jurisdicción civil.

◊¿Si el responsable de un fichero de titularidad privada vulnera el derecho a la protección de datos, la persona afectada puede reclamar responsabilidad simultáneamente por vía administrativa y por vía judicial?

Sí. La persona afectada puede denunciar la infracción ante la Autoridad Catalana de Protección de Datos, por vía administrativa y, de forma simultánea

o con posterioridad, presentar demanda ante el juzgado, por vía judicial, para reclamar daños y perjuicios.

Normativa aplicable: art. 19 y 43 y ss. LOPD; 139 y ss. LRJPAC; 1902 CC; 109, 197 y ss. CP; 18 CE.

7.2 Potestad de inspección y de inmovilización de ficheros

Potestad de inspección

Si hay indicios razonables que se ha cometido alguna infracción de las previstas en la LOPD, la Autoridad puede inspeccionar los ficheros y tratamientos de datos personales, con el fin de obtener todas las informaciones necesarias para verificar el cumplimiento de la normativa en materia de protección de datos e iniciar y tramitar el procedimiento sancionador correspondiente.

Concretamente, la Autoridad puede requerir que se presenten o envíen documentos y datos o bien examinarlos en el lugar donde estén depositados. También puede inspeccionar los equipos físicos y lógicos utilizados, para lo cual puede acceder a los locales donde estén instalados.

Los funcionarios que ejercen la función inspectora tienen la consideración de autoridad pública, están vinculados por el deber de secreto en sus actuaciones y tienen que contar con el auxilio, preferente y urgente, de las entidades inspeccionadas.

Los hechos constatados por los funcionarios de la Autoridad y formalizados en documento público tienen valor probatorio, sin perjuicio de las otras pruebas que puedan aportar las personas interesadas.

Normativa aplicable: art. 40 LOPD; art. 5. j) y 19 LACPD.

Potestad de inmovilización de ficheros

En supuestos de infracción grave o muy grave, en caso de utilización o de comunicación ilícita de datos personales en que se atente gravemente contra los derechos fundamentales y las libertades públicas de los ciudadanos o se impida su ejercicio, la Autoridad puede exigir a los responsables de los ficheros que cesen en esta utilización o comunicación ilícita.

Si no se atiende el requerimiento, los ficheros se pueden inmovilizar para restaurar los derechos de las personas afectadas. La inmovilización queda sin efecto si en el plazo de 15 días hábiles no se acuerda la incoación de un procedimiento sancionador y no se ratifica la medida.

Normativa aplicable: art. 49 LOPD; 25 LACPD.

7.3 Infracciones

El artículo 44 de la LOPD tipifica las infracciones en que pueden incurrir los responsables de los ficheros y los encargados del tratamiento, que pueden ser **leves, graves y muy graves**:

Infracciones leves
No enviar a la APDCAT las notificaciones previstas en la LOPD o en el RLOPD (44.2.a)
No pedir la inscripción del fichero al Registro de Protección de Datos (44.2.b)
Incumplir el deber de información a la persona afectada sobre el tratamiento de sus datos personales, cuando se recogen de la misma persona interesada (44.2.c)
Transmitir datos a un encargado del tratamiento sin cumplir con los deberes formales del art. 12 LOPD (44.2.d)

Infracciones graves
Crear ficheros de titularidad pública o iniciar la recogida de datos sin autorización de disposición general publicada en el DOGC o BOP correspondiente (44.3.a)
Tratar datos sin el consentimiento de la persona afectada, cuando sea necesario obtenerlo según la LOPD y el RLOPD (44.3.b)
Tratar datos o utilizarlos con conculcación de los principios y garantías establecidas en el art. 4 LOPD y en el RLOPD, a menos que constituya una infracción muy grave (44.3.c)
Vulnerar el deber de guardar secreto a que se refiere el art. 10 LOPD (44.3.d)
Impedir u obstaculizar el ejercicio de los derechos ARCO (44.3.e)
Incumplir el deber de información a la persona afectada sobre el tratamiento de sus datos, cuando no se han conseguido de la misma persona interesada (44.3.f)
Incumplir el resto de deberes de notificación o requerimiento de la persona afectada impuestos por la LOPD y el RLOPD (44.3.g)
Mantener los ficheros, locales, programas o equipos que contienen datos sin las condiciones de seguridad que determina el RLOPD (44.3.h)
No atender requerimientos o advertencias de la APDCAT o no proporcionarle todos los documentos o información que solicita (44.3.i)
Obstruir el ejercicio de la función inspectora (44.3.j)
Comunicar o ceder los datos sin contar con legitimación para hacerlo, de acuerdo con la LOPD y el RLOPD, a menos que constituya una infracción muy grave (44.3.k)
Infracciones muy graves
Recoger datos de manera engañosa o fraudulenta (44.4.a)
Tratar o ceder datos especialmente protegidos (apartados 2,3 y 5 del art. 7 LOPD), salvo los supuestos en que la LOPD lo autoriza, o violentar la prohibición del artículo 7.4 LOPD (44.4.b)
No cesar el tratamiento ilícito, cuando hay requerimiento previo del director de la APDCAT (44.4.c)
Transferir datos a países que no proporcionan un nivel de protección equiparable sin autorización de la AEPD, a menos que no sea necesaria según la LOPD o el RLOPD (44.4.d)

Las infracciones previstas en la LOPD prescriben en los plazos siguientes:

a) Infracciones **leves**: un año

b) Infracciones **graves**: dos años

c) Infracciones **muy graves**: tres años

El plazo de prescripción de las infracciones empieza a contar el día en que se ha cometido la infracción. Se interrumpe cuando se inicia el procedimiento sancionador con conocimiento de la persona interesada y se reprende si el expediente está paralizado durante más de seis meses por causa no imputable al presunto infractor.

Normativa aplicable: art. 44, 46 y 47 LOPD.

7.4 Sanciones

Con respecto a las infracciones cometidas en relación con los ficheros de titularidad privada o con información que tendría que estar incluida en ficheros de esta naturaleza, la comisión de una infracción tipificada en la LOPD comporta, junto con el requerimiento para que se adopten las medidas correctoras apropiadas, la imposición de la sanción correspondiente:

a) Infracciones **leves**: multa de 900 a 40.000 €

b) Infracciones **graves**: multa de 40.001 a 300.000 €

c) Infracciones **muy graves**: multa de 300.001 a 600.000 €

De forma excepcional, en supuestos en que no hay reincidencia y siempre que concurran determinadas circunstancias (que la infracción sea leve o grave y que concurran significativamente las circunstancias previstas en el artículo 45.5 LOPD), la Autoridad puede formular una advertencia e imponer al responsable que adopte determinadas medidas correctoras, en lugar de imponer una sanción económica.

Con respecto a las infracciones cometidas en relación con ficheros de **titularidad pública**, no comportan la imposición de ningún tipo de sanción. En este caso, la Autoridad dicta una resolución en que declara la infracción y establece las medidas que hay que adoptar para que cesen o se corrijan los efectos de la infracción. En este caso, la Autoridad también puede proponer que se inicien actuaciones disciplinarias, si son procedentes.

Las sanciones previstas en la LOPD prescriben en los plazos siguientes:

a) Sanciones por infracciones leves: un año.

b) Sanciones por infracciones graves: dos años.

c) Sanciones por infracciones muy graves: tres años.

El cómputo del plazo de prescripción de las sanciones empieza al día siguiente del día en que adquiere firmeza la resolución sancionadora. Se interrumpe cuando se inicia el procedimiento de ejecución con conocimiento de la persona interesada y se reprende si el procedimiento de ejecución está paralizado durante más de seis meses por una causa no imputable al infractor.

Normativa aplicable: art. 37. g), 45-47 LOPD; 5.k), 18, 21-24 LACPD.

7.5 El procedimiento sancionador

La Autoridad Catalana de Protección de Datos, cuando tramita los procedimientos sancionadores y también los procedimientos de declaración de infracciones cometidas en relación con ficheros de titularidad pública, tiene que seguir el procedimiento sancionador aplicable a los ámbitos de competencia de la Generalitat.

Información previa: antes de iniciar el procedimiento, se pueden llevar a cabo actuaciones previas para determinar si se dan circunstancias que justifiquen la incoación.

Si de las actuaciones previas no se derivan hechos susceptibles de no motivar la imputación de ninguna infracción, se dicta resolución de archivo. Si hay indicios susceptibles de motivar la imputación de una infracción, se dicta acuerdo de inicio del procedimiento.

Iniciación: el procedimiento se inicia de oficio, ya sea por denuncia o como consecuencia de informaciones conocidas directamente por la Autoridad.

Notificación y publicación de la resolución: en el caso de infracciones cometidas en relación con ficheros de titularidad pública, la resolución se tiene que notificar a la persona responsable del fichero o del tratamiento, al encargado del tratamiento, si procede, al órgano del cual dependan y a las personas afectadas, si las hay.

En el caso de infracciones cometidas con relación a ficheros de titularidad privada, se notifica a la persona responsable del fichero o del tratamiento, al encargado del tratamiento, si procede, y a las personas afectadas, si las hay.

La persona denunciante tiene derecho que se la informe de las actuaciones que se derivan de la denuncia, sin perjuicio de sus derechos como persona interesada.

Una vez notificada a las personas interesadas, la resolución se hace pública en el web de la Autoridad, previa anonimización de los datos de carácter personal, a menos que no tenga ningún interés doctrinal o que, a pesar de la anonimización, sea aconsejable por causas justificadas evitar la publicidad para impedir que determinadas personas resulten reconocibles. También se comunica al Síndic de Greuges si se dicta en relación con una administración pública.

Régimen de recursos: las resoluciones sancionadoras y de declaración de infracción de la Autoridad agotan la vía administrativa y son susceptibles de recurso de reposición o directamente recurso contencioso administrativo.

Normativa aplicable: art. 37. g), 43, 46 y 48 LOPD; 3.c), 5.k), 17, 18, 19, 21 y ss. LACPD; Decreto 278/1993.

8 Los códigos tipo

Las medidas proactivas, como la aprobación de códigos tipo, facilitan el cumplimiento de la normativa de protección de datos y mejoran la confianza de los ciudadanos en el tratamiento de sus datos

Las previsiones establecidas de forma general en la normativa de protección de datos, se tienen que adaptar a las características y a las necesidades de cada tipo de entidad. Eso se puede hacer mediante los códigos tipo. Este mecanismo de autorregulación, que en este caso pueden promover tanto el Departamento de Enseñanza como los mismos centros, establece la forma como se tienen que cumplir los principios, las obligaciones y las garantías establecidas en la normativa, así como los compromisos adicionales que se consideran necesarios para garantizar mejor los derechos de los ciudadanos.

Los códigos tipo son **acuerdos sectoriales**, **convenios o decisiones de empresa**, mediante los cuales los responsables de los tratamientos pueden establecer, entre otros aspectos, las condiciones de organización, el régimen de funcionamiento, los procedimientos aplicables, las normas de seguridad, las obligaciones de las personas afectadas y las garantías para ejercer sus derechos en materia de protección de datos. Tienen carácter de códigos deontológicos o de buena práctica profesional y son vinculantes para los entes que se adhieren a ellos.

Su objetivo es adecuar las previsiones establecidas en la LOPD y en el RLOPD a los tratamientos que hacen las entidades cuando ejercen su actividad, para armonizarlos mediante reglas, protocolos o estándares, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de la normativa.

Los **centros educativos** pueden adoptar códigos tipo, de acuerdo con lo que establecen las normas que les sean aplicables. El código puede ser del ámbito de un centro o de diversos centros.

Tienen que incluir **procedimientos de supervisión**, para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un **régimen sancionador** que sea adecuado, eficaz y disuasivo.

Estos acuerdos o convenios, cuando afectan exclusivamente centros del ámbito territorial de Cataluña, se tienen que **depositar e inscribir** en el Registro de Protección de Datos de Cataluña.

Una vez inscritos, las entidades están obligadas a:

- Mantener accesible al público información actualizada sobre las entidades promotoras, los adheridos, los procedimientos de adhesión, el contenido y los procedimientos de garantía de cumplimiento.
- Hacer una memoria anual relativa, entre otros aspectos, a la difusión del código, la promoción de su adhesión y las actuaciones para verificar el cumplimiento.
- Evaluar periódicamente su eficacia.

Normativa aplicable: art. 32 LOPD; 71 y ss. RLOPD; 11.2.b) LACPD.

9 Videovigilancia

Las imágenes que captan los sistemas de videovigilancia también son datos personales

La captación de imágenes de personas físicas o su voz mediante cámaras u otros dispositivos electrónicos que las hagan identificables también constituye un tratamiento de datos personales, que tiene sus propias especificidades.

Videovigilancia

Captación de imágenes, y si procede, de voces, a través de un sistema de cámaras fijas o móviles que tengan como objetivo la vigilancia o el control en edificios, instalaciones, vehículos u otros espacios públicos o privados, por razones de seguridad pública o privada, control de tráfico, control laboral, aseguramiento del normal funcionamiento de determinados servicios públicos, control de los hábitos, la conducta o el estado de las personas o por otras razones análogas.

La captación de la imagen con finalidades de videovigilancia está regulada por la Instrucción 1/2009, de la Agencia Catalana de Protección de Datos, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

9.1 Legitimidad y proporcionalidad de la medida

La instalación de sistemas de videovigilancia en los centros educativos se tiene que valorar con especial cuidado dado que puede interferir no sólo en el derecho del alumno a desarrollar su personalidad aprendiendo y expresándose en un entorno no sometido a vigilancia continuada, sino también en la libertad de enseñanza.

Puede ser admisible utilizar cámaras de videovigilancia con la finalidad de salvaguardar la seguridad de las personas (violencia en el centro, control de la entrada y salida de personas del centro) o los bienes (robos, hurtos, degradación de material o de las dependencias del centro). Ahora bien, la adopción de este tipo de medidas tiene que resultar proporcionada a la finalidad que se persigue. Puede ser útil para eso utilizar el test de proporcionalidad:

- Tiene que ser una medida necesaria para conseguir un objetivo determinado, concreto y legítimo.
- No tiene que haber otros medios menos intrusivos para los derechos de las personas.
- La medida tiene que comportar más beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto.

A estos efectos hay que tener en cuenta que puede resultar proporcionado, en relación con las finalidades mencionadas, la captación de imágenes perimetrales del recinto, de los puntos de entrada y salida o de espacios abiertos o accesos a las aulas y dependencias. En cambio, los sistemas de videovigilancia pueden resultar desproporcionados en:

- Espacios como baños, servicios, vestuarios, enfermería etc.
- Salas de profesores, salas de ocio o de descanso de los docentes.
- Espacios como aulas, gimnasios o espacios de ocio del alumnado.

En cualquier caso, la evaluación de la proporcionalidad de la medida obliga a analizar también los aspectos temporales de la captación de imágenes (periodo de instalación, lapsos temporales de captación, periodo de conservación, etc.), a fin de que resulte adecuada a la problemática que se pretenda afrontar.

Así, por ejemplo, si se pretende hacer frente a robos que se puedan producir en horas en que el centro permanece cerrado, no hace falta que funcione durante el horario lectivo. Igualmente, si con la utilización de la videovigilancia se pretende hacer frente a algún problema puntual, la necesidad de la medida puede desaparecer una vez se haya resuelto.

También hay que aplicar este principio al lapso de tiempo en que se conserven las imágenes. Las imágenes sólo se tienen que conservar durante el tiempo indispensable para alcanzar la finalidad perseguida que, en principio, no tiene que ser superior a un mes.

Con respecto a las cámaras exteriores, hay que tener en cuenta que la captación de imágenes de la vía pública para vigilancia de edificios o instalaciones sólo es legítima si es incidental y resulta inevitable para alcanzar la finalidad de vigilancia del edificio o la instalación. Por lo tanto, hay que adecuar el ángulo de visión de las cámaras para evitar que capten imágenes de personas o vehículos identificables que circulen por la vía pública.

9.2 Obligaciones del responsable

Corresponde al responsable:

- Velar por la legitimidad del tratamiento, el contenido del deber de información, con respeto a los principios de calidad, proporcionalidad y finalidad del tratamiento.
- Crear y notificar el fichero al registro de la Autoridad Catalana de Protección de Datos, a menos que los datos se capten pero no se registren.
- Garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición a los titulares de los datos.
- Informar de forma clara y permanente sobre la existencia de las cámaras, aunque las imágenes captadas no se registren, mediante la colocación de los carteles informativos necesarios para garantizar su conocimiento y facilitar la información complementaria que haga falta, de acuerdo con lo que establece el artículo 12 de la Instrucción 1/2009.
- Aplicar las medidas de seguridad apropiadas, de acuerdo con lo que establece el RLOPD y la Instrucción 1/2009.

◊¿Se pueden instalar cámaras en las aulas o en las zonas de esparcimiento del centro educativo, para controlar a los alumnos?

La instalación de las cámaras tiene que cumplir con el principio de proporcionalidad. Instalarlas en estos espacios, sin un bien jurídico superior que lo justifique o si se puede disponer de medios alternativos menos intrusivos para la privacidad de los alumnos y profesores, puede resultar desproporcionado.

◊¿Se pueden utilizar las cámaras de videovigilancia instaladas para la seguridad en los accesos del centro educativo, para el control laboral de los trabajadores del centro?

Si las cámaras se colocan por motivos de seguridad, la instalación está legitimada de acuerdo con el artículo 6.2 LOPD, pero no se pueden utilizar las imágenes para otras finalidades diferentes de las que se hayan establecido en el momento de la aprobación del fichero, como para controlar a los trabajadores del centro.

◊¿Qué medidas de seguridad hay que aplicar a los ficheros de videovigilancia?

De acuerdo con el art. 20.2 de la Instrucción 1/2009, los ficheros de videovigilancia requieren, con carácter general, el nivel de seguridad básico, sin perjuicio que en determinados supuestos, si es previsible captar datos especialmente protegidos, se tienen que aplicar medidas de seguridad de nivel medio o alto.

◊¿En qué casos se tienen que hacer copias de seguridad en los ficheros de videovigilancia?

Si los datos se guardan por un periodo superior a una semana, hay que hacer copias de seguridad semanalmente, de acuerdo con lo que dispone el artículo 21.4.e) de la Instrucción 1/2009.

◊¿Durante cuánto de tiempo se pueden conservar las imágenes obtenidas a través de un sistema de videovigilancia?

Con carácter general, se recomienda que no se exceda el plazo máximo de un mes para cancelar las imágenes.

◊¿La normativa de protección de datos impide que los padres registren imágenes en actos del centro donde participan sus hijos junto con otros niños?

No. La captación de imágenes de los propios hijos en estas circunstancias se puede considerar como una finalidad familiar o doméstica, excluida del ámbito de aplicación de la LOPD (2.2.a) LOPD), si la captación de las imágenes de otros niños es accesoria y no se utilizan con otras finalidades que no sean de carácter doméstico.

Normativa aplicable: art. 8.2.c) LO 1/1982; 5.1.f) RLOPD; Instrucción 1/2009; CNS 44/2010.

10 El tratamiento de datos por el AMPA

Las asociaciones de padres y madres de alumnos son responsables de la información personal que tratan

Las asociaciones de madres y padres de alumnos (AMPA) se pueden constituir, con personalidad jurídica propia, en los centros docentes que imparten enseñanzas en los niveles de educación infantil, primaria, secundaria, bachillerato, formación profesional y otras enseñanzas regladas de nivel no universitario, con la finalidad esencial de facilitar la participación de las madres y los padres en las actividades del centro, además de las establecidas por la normativa vigente y las que determinen los estatutos de dichas asociaciones.

Para ejercer sus funciones, que incluyen, entre otras, la representación y la participación de los padres en la gestión del centro, promover actividades de formación de los padres o, en general, la colaboración del centro en el ámbito social, cultural, económico y laboral del entorno, las AMPA pueden tener que tratar datos de carácter personal tanto de alumnos, de los padres y madres de alumnos, de los cargos de la asociación, de las personas que prestan servicios al AMPA o, en general, de terceras personas con las cuales se relacionan.

Las AMPA pueden tener que tratar datos identificativos, de características personales, académicas y socioeconómicas, entre otros, y en algunos casos también datos especialmente protegidos. Para recoger estos datos, tienen que contar con el consentimiento de las personas afectadas –que tiene que ser expreso, si son datos especialmente protegidos– a menos que alguna norma legal les habilite para hacerlo sin necesidad del consentimiento.

Toda esta información personal se tiene que tratar de acuerdo con la normativa de protección de datos de carácter personal. Por lo tanto, los principios, las obligaciones y las garantías del derecho a la protección de datos que se exponen en los diferentes apartados de esta Guía son de aplicación a las AMPA, a lo cual nos remitimos plenamente. No obstante, hay algunos aspectos específicos que conviene tratar de forma diferenciada.

◊¿El AMPA puede conservar los datos relativos a madres y padres de alumnos que ya no forman parte del centro educativo?

Una vez los datos dejan de ser necesarios para la finalidad para la cual se recogieron, se tienen que cancelar. No obstante, se pueden conservar debidamente bloqueados, de acuerdo con el apartado 6 de esta Guía, mientras no hayan prescrito las responsabilidades que se hayan podido generar durante el tratamiento.

10.1 El responsable del fichero

Tal como hemos visto en el apartado 2.3 de esta Guía, el responsable del tratamiento o del fichero es quien decide sobre la finalidad, el uso y el contenido del tratamiento. El responsable de los ficheros de datos de carácter personal que tenga que crear el AMPA es el órgano de ésta que se determine.

Como responsable, el AMPA tiene todas las obligaciones que se derivan: informar a las personas sobre la finalidad con que se tratan los datos y los otros aspectos que requiere la normativa, velar por el cumplimiento del deber de confidencialidad, atender el ejercicio de los derechos ARCO o adoptar las medidas de seguridad apropiadas, entre otros. Por lo tanto, es el AMPA quien tiene que responder de las responsabilidades que se pueden derivar de los tratamientos de datos que lleve a cabo.

10.2 La creación y la notificación de los ficheros del AMPA

Vistas sus funciones, las AMPA tienen que disponer como mínimo de un fichero para recoger información personal relativa a sus asociados, así como a sus órganos de gobierno. Más allá de eso, y de acuerdo con las actividades que despliegue cada AMPA, puede que se necesite crear otros ficheros para otras finalidades específicas que no tengan cabida en la finalidad que el AMPA haya establecido para este fichero.

Considerando que las AMPA son asociaciones y que, por lo tanto, tienen naturaleza jurídica privada, sus ficheros son de titularidad privada.

En consecuencia, su creación no está sometida a un procedimiento formal específico, sino que es suficiente que, antes de empezar a recoger los datos, la asociación lo acuerde y se notifique al Registro de Protección de Datos de Cataluña de la Autoridad Catalana de Protección de Datos.

Estas mismas consideraciones son aplicables con respecto a la modificación y la supresión de los ficheros.

◊¿Qué naturaleza tienen los ficheros de una AMPA?

Las AMPA son asociaciones con personalidad jurídica propia, y sus ficheros son de naturaleza privada, ya que su responsable es una entidad jurídicoprivada, de acuerdo con lo que establece el artículo 5.1.l) RLOPD.

◊¿Dónde se tienen que notificar e inscribir los ficheros del AMPA de un centro concertado?

Antes de empezar a tratar los datos, el AMPA de los centros concertados de Cataluña tiene que notificar sus ficheros al Registro de Protección de Datos de Cataluña, al encontrarse dentro del ámbito competencial de la Autoridad Catalana de Protección de Datos, de acuerdo con el artículo 3. h) LACPD.

10.3 Comunicaciones de datos

En el momento de comunicar la información personal que consta en sus ficheros, el AMPA está sometida a las mismas limitaciones que se exponen, con carácter general, en el apartado 5.2 de esta Guía.

Conviene tener presente que los ficheros del AMPA no forman parte de los ficheros del centro, ni al revés. Por lo tanto, el centro no puede acceder a los ficheros del AMPA. Y, de la misma manera, el AMPA no puede tratar los datos que figuran en los ficheros del centro, a menos que en uno y otro caso concurra alguna de las circunstancias a que se refiere el apartado 5.2 de esta Guía.

Si el despliegue de la actividad del AMPA requiere que determinado personal del centro acceda a los ficheros del AMPA, por ejemplo para prestar apoyo administrativo o soporte informático, o para que el AMPA pueda utilizar dependencias o equipos informáticos del centro para tratar datos personales, conviene que ambas entidades establezcan previamente un contrato o acuerdo de encargo del tratamiento. Este acuerdo tiene que establecer los términos en que se accederá, el deber de confidencialidad respecto de la información en el cual se acceda, la imposibilidad de utilizar la información personal para otra finalidad diferente a aquélla para la cual se haya hecho el encargo y el resto de aspectos a que se refiere el artículo 12 de la LOPD.

Si el AMPA contrata otros servicios con terceras personas (por ejemplo para las actividades extraescolares) que comportan el acceso a datos personales de los ficheros del AMPA, también hay que establecer un acuerdo de encargo, con la entidad de que se trate.

Sobre todas estas cuestiones consultar el apartado 5.3 de esta Guía.

◊¿Un colegio puede facilitar al AMPA un listado de las direcciones electrónicas de los padres de los alumnos?

No. No hay ninguna norma legal que habilite esta comunicación y, por lo tanto, hace falta el consentimiento de los padres para que el centro educativo pueda ceder los datos. Esta comunicación no está amparada en ninguna de las excepciones del artículo 11 LOPD.

◊¿El AMPA puede difundir en su blog imágenes de las actividades realizadas?

Si en las imágenes aparecen personas identificables, el AMPA necesita el consentimiento de las personas afectadas, a menos que se hayan captado en un acto público y la imagen de la persona aparezca como meramente accesoria, o que se cuente con otra habilitación legal.

◊¿La junta del AMPA puede difundir al resto de miembros del AMPA el contenido de una queja dirigida específicamente a la Junta sobre una actuación del centro educativo?

Si la queja manifiesta expresamente que quiere poner en conocimiento de la junta unos hechos determinados y de la misma no se desprende la voluntad que sea difundida a otros miembros de la asociación, hay que evitar la difusión. Eso sin perjuicio de poder llevar a cabo las acciones apropiadas ante el centro en relación con el motivo de la queja.

Si la queja puede ser de interés de otros padres de alumnos, hace falta obtener el consentimiento de la persona afectada o anonimizarla, eliminando los elementos que puedan hacer identificables a las personas implicadas.

10.4 Ejercicio de derechos

En el caso de los datos que trata el AMPA, las personas afectadas también disfrutan de los derechos de acceso, rectificación, cancelación y oposición, que se tienen que ejercer ante del órgano del AMPA, establecido en el momento de la creación del fichero.

Sobre el ejercicio de estos derechos, consultar el apartado 5.5 de esta Guía.

◊¿Delante de quién se tiene que ejercer el derecho de acceso con respecto a las actividades extraescolares organizadas y gestionadas por el AMPA?

El derecho de acceso se tiene que ejercer delante del responsable del tratamiento de los datos, que en este caso sería el AMPA como organizadora de las actividades.

◊¿Si una AMPA recibe una solicitud de baja a la asociación y cancelación de los datos del padre de un alumno, es suficiente darlo de baja como asociado?

No. La respuesta tiene que resolver también la solicitud de cancelación.

10.5 Medidas de seguridad

Como responsable de los ficheros, el AMPA tiene que elaborar el documento de seguridad, adoptar las medidas de seguridad correspondientes y velar para que se apliquen correctamente, de acuerdo con lo que se ha expuesto en el apartado 5.6 de esta Guía.

Conviene, sin embargo, hacer especial atención a los aspectos siguientes:

- Adoptar las medidas adecuadas para que la información que sea responsabilidad del AMPA esté debidamente custodiada. Siempre que sea posible, la información tiene que estar en equipos o espacios bajo el control exclusivo del AMPA y evitar el traslado a domicilios o equipos particulares de las personas que forman parte. Hay que prestar especial atención a la destrucción o al rechazo de la información que puede contener datos de carácter personal y de los soportes donde figura, con el fin de evitar que terceros accedan a ella.
- Separar la información que forma parte de los ficheros del AMPA respecto de la que forma parte de los ficheros del centro educativo. Si se comparten espacios físicos o incluso equipos informáticos conviene que cada responsable disponga de sus propias medidas de seguridad que permitan compartimentar, de manera eficaz y confidencial, su información.
- Planificar con antelación todos los aspectos que afectan a la continuidad en la custodia y el tratamiento de la información, vistas las particulares circunstancias de las AMPA, que a menudo no cuentan con personal propio y en los cuales los cargos van cambiando con cierta frecuencia. En este sentido, puede ser útil prever con antelación el protocolo para el proceso de revocación y dada de alta de permisos para acceder a la información, que se tiene que hacer lo antes posible a partir del momento en que se modifique la situación que justifica que una persona esté como usuaria.

Normativa aplicable: art. 3.d) LOPD; 3. h) LACPD; 118.3 y 4, 119.1 y 2, 121.5, 126.1.e) LOE; 5.1.l) RLOPD); Decreto 202/1987; PET 5/2009.

11 La Autoridad Catalana de Protección de Datos

La Autoridad Catalana de Protección de Datos es la autoridad de control competente con respecto a los ficheros y tratamientos de datos de carácter personal de los centros educativos públicos y concertados de Cataluña

11.1 Naturaleza y objeto

La Autoridad Catalana de Protección de Datos, entidad sucesora de la Agencia Catalana de Protección de Datos, es un organismo independiente, designado por el Parlamento de Cataluña, que tiene por objeto garantizar, en el ámbito de las competencias de la Generalitat, los derechos a la protección de datos personales y de acceso a la información a ella vinculada.

Se regula por la Ley 32/2010, del 1 de octubre, de la Autoridad Catalana de Protección de Datos, y el Decreto 48/2003, de 20 de febrero, por el cual se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, vigente en todo lo que no se opone a la ley mencionada.

Se configura como institución de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, con plena autonomía orgánica y funcional, que actúa con objetividad y plena independencia de las administraciones públicas en el ejercicio de sus funciones.

Normativa aplicable: art. 31 y 156.d) EAC; 1 y 2 LACPD.

11.2 Ámbito de actuación

El ámbito de actuación de la Autoridad comprende los ficheros y los tratamientos de las entidades siguientes:

- Las instituciones públicas de Cataluña.
- La Administración de la Generalitat.

- Los entes locales.
- Las entidades autónomas, los consorcios y las otras entidades de derecho público vinculadas a la Administración de la Generalitat o a los entes locales, o que dependen de ellos.
- Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalitat o a los entes locales, o que dependen de ellos:
  – Que su capital pertenezca mayoritariamente a dichos entes públicos.
  – Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos
  – Que en sus órganos directivos los miembros designados por dichos entes públicos tengan mayoría
- Las otras entidades de derecho privado que prestan servicios públicos por medio de cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de estos servicios.
- Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que dependen de él.
- Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalitat o de los entes locales, si se trata de ficheros o tratamientos destinados al ejercicio de estas funciones y el tratamiento se lleva a cabo en Cataluña.
- Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña a los efectos de lo que establece la LACPD (por ejemplo, los colegios profesionales que ejercen sus funciones exclusivamente en Cataluña, tanto con respecto a sus ficheros de titularidad pública como los de titularidad privada).

El EAC prevé que la Generalitat de Cataunya tiene que establecer un modelo de interés público como garantía del derecho de todas las personas a una educación de calidad y a acceder a ella en condiciones de igualdad, a través del Servicio de

Educación de Cataluña, conformado por los centros públicos y privados sostenidos con fondos públicos.

Por lo tanto, **forman parte** del ámbito de actuación de la APDCAT:

- Los centros educativos públicos, en la medida que se trata de centros que son de la titularidad o dependen de la Generalitat de Catalunya o de los entes locales de Cataluña.
- Los centros educativos privados sostenidos con fondos públicos a través de cualquier forma de gestión directa o indirecta de servicios públicos, como el concierto, si se trata de ficheros y tratamientos vinculados a la prestación de estos servicios.
- Los ficheros de las AMPA que se constituyan en los centros educativos mencionados, en la medida en que participan en las funciones públicas educativas que se ejercen en ellos.

No forman parte del ámbito de actuación de la APDCAT los centros educativos privados no concertados, ni las AMPA que se constituyan en ellos, con independencia que puedan recibir algún tipo de subvención finalista que no forme parte del sistema de conciertos previsto en la normativa vigente.

◊¿La fundación creada en el seno de un centro concertado forma parte del ámbito de actuación de la APDCAT?

Sí. Los entes que dependen o están vinculados a entidades u organismos que forman parte del ámbito de actuación de la APDCAT también están incluidos en el ámbito de actuación de la APDCAT.

◊¿Un jardín de infancia privado que recibe subvenciones públicas está incluido dentro del ámbito de actuación de la APDCAT?

Los ficheros del jardín de infancia sólo estarían incluidos dentro del ámbito de actuación de la APDCAT si el jardín de infancia tiene encargada la gestión de un servicio público, por ejemplo a través de la fórmula del concierto o la concesión. El simple hecho de recibir una subvención pública no otorga a esta entidad la consideración de gestor de un servicio público.

◊¿Los consejos escolares deportivos forman parte del ámbito de actuación de la APDCAT?

Sí. Los ficheros de los consejos deportivos están incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos si están vinculados al ejercicio de funciones públicas.

Normativa aplicable: art. 156 EAC; 3 LACPD; CNS 42/2013, PET 5/2009, PET 8/2011, PET 10/2011, PET 6/2012.

11.3 Organización y funciones

Estructura

La Autoridad dispone de dos órganos:

- El/la **director/a**, que dirige la institución y ejerce su representación.
- El **Consejo Asesor de Protección de Datos**, órgano de asesoramiento y participación de la Autoridad, constituido por representantes de las diferentes instituciones incluidas dentro de su ámbito de actuación.

Normativa aplicable: art. 6 y ss. LACPD; 13 y ss. Decreto 48/2003.

Funciones

La Autoridad ejerce, entre otras funciones, las siguientes:

- **Atención al público y consultoría**:

  El servicio de atención al público atiende las solicitudes de información, quejas o consultas sobre los servicios de la Autoridad y sobre la aplicación de la legislación de protección de datos de carácter personal que formule cualquier

ciudadano o el personal de las entidades sometidas en el ámbito de actuación de la Autoridad.

El servicio de consultoría se dirige a los responsables de los ficheros y de los tratamientos y a los encargados del tratamiento, para prestarles apoyo en los procesos de notificación de ficheros, en la adecuación de los tratamientos a la normativa de protección de datos personales y en la aplicación de las medidas de seguridad.

Se puede contactar con estos servicios a través de:

- Teléfono: 902 011 710 (de 9 a 14 h, de lunes a viernes laborables).
- Por correo electrónico: consultes.apdcat@gencat.cat.
- Por correo postal: calle de la Llacuna, 166, 7ª planta, 08018 Barcelona.
- Por fax: 93 552 78 30.
- Presencialmente: de 9 a 14 h, de lunes a viernes laborables.

- **Difusión** del derecho a la protección de datos de carácter personal mediante publicaciones, conferencias, cursos, seminarios y otras iniciativas. A estos efectos, la Autoridad dispone de una lista de distribución sobre sus iniciativas, la inscripción a la cual se puede solicitar enviando un correo electrónico dirigido a consultes.apdcat@gencat.cat.
- **Registro:** inscripción a través del Registro de Protección de Datos de Cataluña de:
  a) Los ficheros, de titularidad pública o privada, incluidos dentro del ámbito de actuación de la Autoridad.
  b) Los códigos tipo formulados por las entidades incluidas dentro del ámbito de actuación de la Autoridad.
- **Elaboración de informes** sobre los proyectos de disposiciones de carácter general o acuerdos de creación, modificación o supresión de ficheros y sobre disposiciones que tengan impacto en materia de protección de datos de carácter personal. En el caso de la Administración de la Generalitat y los centros que dependen de ella, estos informes son preceptivos.

- **Elaboración de dictámenes** en relación con las consultas que formulan los representantes de las entidades de su ámbito de actuación.
- **Elaboración de recomendaciones e instrucciones**, para adecuar los ficheros y los tratamientos de datos a los principios y a las garantías que establece la legislación vigente de protección de datos.
- **Tutela de los derechos ARCO**, mediante un procedimiento de reclamación dirigido a hacer efectivos y restablecer de forma inmediata estos derechos de los ciudadanos.
- **Funciones de control**, mediante:
  a) Los planes de auditoría, como sistema de control preventivo para verificar el cumplimiento de la normativa y recomendar o requerir a los responsables de los ficheros y tratamientos que adopten las medidas correctoras adecuadas.
  b) La potestad de inspección, por la cual la Autoridad puede inspeccionar los ficheros y los tratamientos de datos personales, para obtener la información necesaria para desarrollar su actividad.
  c) La aplicación del régimen sancionador previsto en la LOPD respecto de los responsables de los ficheros y de los tratamientos incluidos dentro del ámbito de actuación de la Autoridad, y de los encargados de los tratamientos correspondientes.
  d) Los requerimientos de adecuación a la legalidad, en caso de infracciones graves o muy graves, para exigir el cese de la utilización o la comunicación ilícita de datos personales y, si procede, la potestad de inmovilización de ficheros, en caso de incumplimiento de los requerimientos de adecuación.
- **Otorgar autorizaciones**, para la exención del deber de información en la recogida de los datos o para el mantenimiento íntegro de determinados datos, y otros que establezca la normativa, salvo las relativas a transferencias internacionales de datos, que son competencia del director de la Agencia Española de Protección de Datos.

Norma aplicable: art. 5 y 15 y ss. LACPD.

Abreviaturas

AMPA: Asociación de madres y padres de alumnos

APDCAT: Autoridad Catalana de Protección de Datos

CC: Código civil

CCC: Ley 25/2010, del 29 de julio, del libro segundo del Código Civil de Cataluña, relativo a la persona y la familia

CE: Constitución Española

CNS: dictamen emitido por la APDCAT

Decreto 202/1987: Decreto 202/1987, de 19 de mayo, por el cual se regulan las asociaciones de padres de alumnos

Directiva 95/46/CE: Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de estos datos

Derechos ARCO: derecho de acceso, rectificación, cancelación y oposición

EAC: Estatuto de autonomía de Cataluña

Instrucción 1/2009: Instrucción 1/2009 de 10 de febrero, de la Agencia Catalana de Protección de Datos, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia

LACPD: Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos

LE: Ley 12/2009, de 10 de julio, de educación

Llei 10/2001: Ley 10/2001, de 13 de julio, de archivos y documentos

LODE: Ley orgánica 8/1985, de 3 julio, reguladora del derecho a la educación

LOE: Ley orgánica 2/2006, de 3 de mayo, de educación

LOPD: Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

LO 1/1982: Ley orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen

LRBRL: Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local

LRJPAC: Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común

LTAIPBG: Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

Ordre EDU/316/2010: Orden EDU/316/2010, de 27 de mayo, de creación del fichero de datos de carácter personal Proyecto eduCAT 1x1 gestionado por el Departamento de Educación

Ordre ENS/125/2011: Orden ENS/125/2011, de 13 de mayo, de actualización de los ficheros que contienen datos de carácter personal gestionados por el Departamento de Enseñanza

Ordre ENS/59/2014: Orden ENS/59/2014, de 28 de febrero, de regulación de ficheros que contienen datos de carácter personal del Departamento de Enseñanza

PD: Informe emitido por la APDCAT

PET: Informe emitido por la APDCAT

Recomanación 1/2010: Recomendación 1/2010 de la Agencia Catalana de Protección de Datos sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña

Recomanación 1/2011: Recomendación 1/2011 de la Autoridad Catalana de Protección de Datos sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública

RLOPD: Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real decreto 1720/2007, de 21 de diciembre

TRLCSP: Texto refundido de la Ley de contratos del sector público, aprobado por el Real decreto legislativo 3/2011, de 14 de noviembre