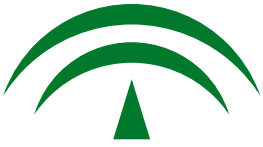
GUÍA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL PARA LOS CENTROS DE ENSEÑANZA

(LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, Y REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE)



CONSEJERÍA DE EDUCACIÓN

Isidro Gómez-Juárez Sidera.
Consultor, Auditor y Formador en Protección de Datos de Carácter Personal. DEA en Derecho de las Nuevas Tecnologías de la Información y las Comunicaciones.

Francisco Silveira García.
Jefe de Sistemas de Información.

Elías Fernández Martín.
Servicio de Sistemas de Información.

Servicio de Legislación, Recursos y Relaciones con la Administración de Justicia de la Consejería de Educación.

Revisión: Agenda Activa

Edita:Junta de Andalucía
Consejería de Educación

ISBN: 978-84-690-6607-2

Depósito Legal: SE-3341-2011

Diseño: RRM

Impresión: Coria Gráfica, S. L.

PRESENTACIÓN

El derecho a la protección de datos: un derecho fundamental del alumnado.

La Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989 y aprobada por España mediante Instrumento de Ratificación de 30 de noviembre de 1990, consagró en su artículo 3 el principio jurídico fundamental del interés superior de los niños y niñas: *"En todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los Tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño"* (art. 3.1). En este sentido, los Estados partes se comprometieron *"a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la Ley y, con ese fin, tomarán todas las medidas legislativas y administrativas adecuadas"* (art. 3.2).

El citado principio ha confirmado su solidez a través de la Carta de los Derechos Fundamentales de la Unión Europea, cuyo artículo 24, relativo a los *"Derechos del menor"*, establece que *"en todos los actos relativos a los menores llevados a cabo por autoridades públicas o instituciones privadas, el interés superior del menor constituirá una consideración primordial"* (art. 24.2).

En nuestro país, la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, también recoge el principio del interés superior del menor como un principio general que debe primar sobre cualquier otro en su aplicación: *"En la aplicación de la presente Ley primará el interés superior de los menores sobre cualquier otro interés legítimo que pudiera concurrir"* (art. 2, párrafo primero). Asimismo, la citada Ley establece que será principio rector de la actuación de los poderes públicos, entre otros, *"la supremacía del interés del menor"* (art. 11.2.a)). Finalmente, es importante recordar que de acuerdo con lo señalado en el artículo 4.1 de la Ley Orgánica 1/1996, *"los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen"*.

Conforme a lo establecido en el artículo 18 de la Constitución Española de 1978, enmarcado dentro de la Sección 1ª del Capítulo Segundo del Título I, que lleva por rúbrica *"De los derechos fundamentales y de las libertades públicas"*, los derechos al honor, a la intimidad personal y familiar y a la propia imagen tienen el rango de fundamentales. Asimismo, el apartado 4 del citado artículo establece que *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. El art. 18.4 CE, circunscrito dentro de un precepto dedicado a la protección de la intimidad entendida en sentido amplio, ha sido el eje vertebrador en torno al cual se ha cimentado la normativa española de protección de datos hasta la aparición de la trascendental Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional, que consagró el derecho a la protección de datos de carácter personal como un derecho fundamental autónomo e independiente del derecho a la intimidad.

El contenido del derecho fundamental a la protección de datos consiste, tal y como señala la propia Sentencia 292/2000 en su fundamento jurídico séptimo, *"en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"*. De tal modo, este derecho autónomo e informador de nuestro texto constitucional está integrado por los principios y derechos que se contemplan en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual, a su vez, ha sido objeto de desarrollo reglamentario a través del Real Decreto 1720/2007, de 21 de diciembre. Hay que subrayar que el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea también confiere al derecho a la protección de datos de carácter personal el rango de derecho fundamental, estableciendo que *"toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan"* (art. 8.1).

Por otro lado, si bien los datos de las personas menores de edad no

tienen la consideración jurídica de *"datos especialmente protegidos"* conforme a lo establecido en nuestra normativa nacional de protección de datos de carácter personal, parte de la doctrina entiende que forman parte de una categoría *sui generis* que podría denominarse *"datos de personas especialmente vulnerables"*, basada en un criterio subjetivo en función de las personas titulares de los datos y las especiales condiciones que les rodean. Fruto de la preocupación en relación a los menores, el referido Real Decreto 1720/2007 dedica su artículo 13 a regular de forma específica las cuestiones relativas al consentimiento para el tratamiento de sus datos.

Siguiendo un camino similar, el Grupo de Protección de Datos del artículo 29, órgano europeo consultivo en materia de protección de datos y privacidad, también ha emitido, en fecha 11 de febrero de 2009, un *"Dictamen sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas)"*, con el objetivo de analizar los principios generales que se aplican a la protección de los datos de los niños y niñas, así como explicar su pertinencia en un sector crítico específico como el de los datos escolares. El citado documento debe considerarse en el contexto de la iniciativa general de la Comisión Europea que se describe en la Comunicación *"Hacia una Estrategia de la Unión Europea sobre los Derechos de la Infancia"*: Al contribuir a este objetivo general, pretende reforzar el derecho fundamental de los niños y las niñas a la protección de datos personales, eligiéndose el ámbito escolar por ser uno de los más importantes de la vida del menor, en el que se desarrolla una parte considerable de sus actividades cotidianas, y por la naturaleza confidencial de gran parte de los datos que se tratan en las instituciones de enseñanza. Asimismo, el referido Dictamen se basa en el convencimiento de que la educación y la responsabilidad son instrumentos cruciales para la protección de los datos de los niños y niñas.

En este sentido, el Grupo del artículo 29 ha señalado que *"un niño es un ser humano en el más amplio sentido de la palabra. Por este motivo, debe disfrutar de todos los derechos de la persona, incluido el derecho a la protección de los datos personales. Ahora bien, el niño se encuentra en una situación particular que es preciso considerar desde dos perspectivas: estática y dinámica. Desde el punto de vista estático, el niño es una persona*

que todavía no ha alcanzado la madurez física y psicológica. Desde el punto de vista dinámico, se encuentra en un proceso de desarrollo físico y mental que le convertirá en adulto. Los derechos del niño y su ejercicio -incluido el derecho a la protección de datos- deben expresarse teniendo presentes ambas perspectivas".

De igual manera, entiende que el principio jurídico fundamental que debe regir el tratamiento de los datos de los menores es el interés superior de los mismos, consagrado en la citada Convención de las Naciones Unidas sobre los Derechos del Niño: *"La justificación de este principio es que una persona que todavía no ha alcanzado la madurez física y psicológica necesita más protección que otras personas. Su finalidad es mejorar las condiciones del niño y reforzar el derecho de éste a desarrollar su personalidad. Todas las instituciones, públicas o privadas, que toman decisiones sobre los niños, deben respetar este principio"*. Asimismo, *"hay que reconocer que para alcanzar un nivel adecuado de atención a los niños, los datos personales de éstos deben ser tratados exhaustivamente y por diversas partes. Este tratamiento tendrá lugar principalmente en los sectores del Estado del bienestar: educación, seguridad social, sanidad, etc. Pero esto no es incompatible con la intensificación de una protección adecuada en estos sectores sociales, a pesar de que hay que extremar el cuidado cuando se produce el intercambio de datos sobre los niños".*

Por último, es necesario recordar que la propia Ley Orgánica 2/2006, de 3 de mayo, de Educación, en consonancia con la consolidación del derecho fundamental a la protección de datos de carácter personal, dedica una disposición adicional específica a los datos personales del alumnado, a la cual se remite la Ley 17/2007, de 10 de diciembre, de Educación de Andalucía, publicada en el BOJA núm. 252, de 26 de diciembre de 2007.

En suma, el derecho a la protección de datos de carácter personal se confirma como un derecho fundamental de todo el alumnado, objeto de creciente atención por parte de nuestros legisladores y de los organismos de la Unión Europea. Con el objetivo de contribuir a su difusión, asentamiento y respeto en los centros de enseñanza de la Junta de Andalucía, se elabora la presente guía.

INDICE

CAPÍTULO I

EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En la actualidad, nadie puede permanecer ajeno a las ventajas que han supuesto para todos los sectores sociales y económicos el desarrollo de la informática y la expansión de las telecomunicaciones. La utilización de las nuevas herramientas informáticas en combinación con las redes de telecomunicaciones avanzadas en el ámbito de la Administración Pública está contribuyendo a alcanzar unos mayores grados de eficacia y eficiencia a la hora de gestionar las relaciones y los servicios que éstas prestan a la ciudadanía.

Sin embargo, el uso de la informática y las telecomunicaciones en todos los ámbitos también tiene una vertiente negativa, en el sentido de que su utilización sin las debidas garantías puede afectar a los derechos y libertades individuales de la ciudadanía, en especial en lo referente a su intimidad y a la protección de sus datos.

Consciente de los riesgos derivados de un posible uso inadecuado de estas nuevas tecnologías en detrimento de los citados derechos, la Unión Europea viene realizando, desde hace varios años, un importante esfuerzo de armonización de las legislaciones nacionales de los Estados miembros con el objetivo de que toda la ciudadanía europea cuente con una protección equivalente de alto nivel de sus datos personales en el territorio de la Unión.

Con este propósito, tuvo lugar la aprobación de la 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 y, posteriormente, de la DIRECTIVA 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

En idéntica línea a la emprendida por las dos anteriores, podemos encontrar la más reciente 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, que deroga a la citada Directiva 97/66/CE y

da un paso más en lo relativo a la protección de los datos personales en el ámbito de las telecomunicaciones.

El Tratado por el que se establece una Constitución para Europa tampoco quiso permanecer ajeno a esta cuestión, refiriéndose por dos veces al derecho a la protección de datos de carácter personal: en primer lugar, como un principio que debe inspirar la vida democrática de la Unión (artículo I-51) y, en segundo lugar, elevándolo a la categoría de derecho fundamental, en su artículo II-68 (enmarcado en la Carta de los Derechos Fundamentales de la Unión, que constituye la Parte II del Tratado).

Asimismo, el 28 de enero de 2007 fue el día elegido por el Consejo de Europa para celebrar, por primera vez, el Día Europeo de Protección de Datos. Ésta era una fecha especialmente significativa ya que coincidía con la aprobación en el año 1981 del CONVENIO 108 DEL CONSEJO DE EUROPA, germen del derecho a la protección de datos de carácter personal en la Unión Europea y en cuyos principios se inspira la citada Directiva 95/46/CE. Uno de los principales objetivos del primer Día Europeo de Protección de Datos fue concienciar a la ciudadanía de la Unión sobre sus derechos y obligaciones en lo que a la protección de datos de carácter personal se refiere.

Como contrapunto a este interés normativo, propio del "Viejo Continente", en favor de la protección de los datos de carácter personal de la ciudadanía, la legislación de los Estados Unidos de América, pensada desde el punto de vista de la libertad de empresa y la competitividad en el marco de la economía de mercado, se encuentra entre las menos rigurosas del mundo en la materia.

En este sentido, la presión de los ciudadanos y ciudadanas preocupados por los abusos y las exigencias del mercado ha sido el motor de la aparición de ciertas normas como la Children's Online Privacy Protection Act of 1998, conocida bajo el acrónimo COPPA, elaborada a partir de los trabajos preliminares realizados por el Center for Media Education, organización no gubernamental y sin ánimo de lucro dedicada en Estados Unidos a la creación de una cultura de la calidad en los medios de comunicación digitales dirigidos a los menores y sus familiares. En 1996, su informe llamado

"Web of Deception" llamó la atención sobre la realización de prácticas de marketing y recogida de datos de menores en Internet potencialmente peligrosas para los mismos y sentó las bases para la creación de la COPPA, que marcó un hito regulatorio en lo que a la protección de la privacidad de los menores en la Red se refiere.

En una línea similar, los senadores Ron Wyden y Ted Stevens presentaron, en marzo de 2004, un Proyecto de Ley bajo el nombre de Children's Listbroker Privacy, con el objeto de limitar, a través del consentimiento expreso de los padres, la venta de datos de carácter personal de niños con fines comerciales y de marketing. En este sentido, diversos estudios realizados en el país anglosajón revelaron la existencia de compraventa de información personal de niños de hasta menos de dos años edad. Dicho Proyecto de Ley no llegó a aprobarse definitivamente.

Citar por último que, tras el atentado terrorista del 11-S, la ciudadanía de los Estados Unidos de América ha sido objeto de nuevas limitaciones en lo que al derecho a la protección de sus datos de carácter personal se refiere en favor de la seguridad del Estado.

En España, el derecho a la protección de datos de carácter personal tiene, desde la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, la consideración de derecho fundamental autónomo, siendo, por ende, merecedor de la más elevada protección por parte de nuestro ordenamiento jurídico.

Este derecho informador de nuestro texto constitucional se concreta en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a su posesión o uso.

El texto normativo de referencia en nuestro país en materia de protección de datos personales es la LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, conocida bajo el acrónimo LOPD,

de obligado cumplimiento para toda empresa o Administración Pública que maneje información concerniente a personas físicas identificadas o identificables como consecuencia de las actividades desarrolladas dentro de su objeto social o del ejercicio de sus competencias de carácter público, respectivamente.

Llegar a la actual LOPD ha sido un camino largo y no exento de dificultades, pero que muestra una trayectoria ininterrumpida hacia el asentamiento de una cultura de la protección de datos en todos los sectores de nuestra sociedad y en cualquier ámbito, público y privado.

La primera norma reguladora del derecho a la protección de datos en España fue la LEY ORGÁNICA 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal (en adelante, LORTAD), dictada, con cierto retraso, como consecuencia de la ratificación por España del Convenio 108 del Consejo de Europa. Posteriormente, fruto de la aparición de la Directiva 95/46/CE, se optó por derogar aquélla en lugar de proceder a su modificación, dando paso a la vigente Ley Orgánica 15/1999. Ambas normas (LORTAD y LOPD) tuvieron sus avatares, siendo algunos de sus artículos objeto de sendos recursos de inconstitucionalidad, que dieron lugar a las Sentencias 290/2000 y 292/2000. La segunda de estas sentencias fue la que, como ya hemos dicho, consagró definitivamente en nuestro país el derecho a la protección de datos de carácter personal como un derecho fundamental independiente.

Además, en nuestro país existe un organismo encargado de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, la Agencia Española de Protección de Datos (en adelante, AEPD), dotada de potestades inspectora y sancionadora. La AEPD es un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se rige por lo dispuesto en el Título IV de la LOPD y en Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la AEPD.

Asimismo, la Ley Orgánica 15/1999 establece en su art. 41 que las funciones atribuidas a la Agencia Española de Protección de Datos serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad Autónoma (con la excepción de determinadas funciones concretas que se reservan en exclusiva a la AEPD), que tendrán, al igual que aquélla, la consideración de autoridades de control, a las que se garantizarán plena independencia y objetividad en el ejercicio de su cometido.

De tal manera, en la actualidad existen tres agencias autonómicas de protección de datos creadas al amparo del art. 41 LOPD: La Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), regulada en el Capítulo IV de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, la Agencia Catalana de Protección de Datos (APDCAT), creada por el art. 1 de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos y La Agencia Vasca de Protección de Datos (AVPD), creada por el art. 10 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Agencia de Protección de Datos de la Comunidad de Madrid

apdcat
Agència Catalana de Protecció de Dades

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

En el ámbito concreto de nuestra Comunidad Autónoma, la Ley Orgánica 2/2007, de reforma del Estatuto de Autonomía para Andalucía, contempla en su Título II, bajo la rúbrica general de *"Competencias de la Comunidad Autónoma"*, que *"Corresponde a la Comunidad Autónoma de Andalucía la competencia ejecutiva sobre protección de datos de carácter personal, gestionados por las instituciones autonómicas de Andalucía, Administración autonómica, Administraciones locales, y otras entidades de derecho público y privado dependientes de cualquiera de ellas, así como por las universidades del sistema universitario andaluz"* (art. 82).

El citado artículo abre la puerta a la creación de una Agencia Andaluza de Protección de Datos. La citada Agencia asumiría, entre otras, la función de velar por el cumplimiento de la legislación sobre protección de datos en los centros de enseñanza de la Junta de Andalucía.

Asimismo, el art. 32 del nuevo Estatuto, que lleva por título *"Protección de datos"*, establece que *"se garantiza el derecho de todas las personas al acceso, corrección y cancelación de sus datos personales en poder de las Administraciones públicas andaluzas"*.

CAPÍTULO II

NORMATIVA VIGENTE SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL APLICABLE A LOS CENTROS DE ENSEÑANZA

1. Normativa general

La informatización de los centros de enseñanza a través de herramientas para la gestión de los datos del alumnado, creación de páginas web de los centros donde se publican imágenes de los alumnos y alumnas, e incluso instalación de cámaras de videovigilancia, se une a otra serie de cuestiones que tradicionalmente podían afectar a la intimidad del alumnado, como la confidencialidad de los expedientes académicos o de los informes psicopedagógicos elaborados por los orientadores y orientadoras.

La CONSTITUCIÓN ESPAÑOLA de 1978 garantiza *"el derecho al honor, a la intimidad personal y familiar y a la propia imagen"* (art. 18.1 CE). Asimismo, establece que *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"* (art. 18.4 CE).

El citado art. 18.4 ha sido el pilar fundamental de nuestro sistema de protección de datos hasta la aparición de la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, que consagró el derecho a la protección de datos de carácter personal como un derecho fundamental específico y distinto del derecho a la intimidad.

Partiendo de estas premisas, los centros de enseñanza deben ser plenamente conscientes de que el alumnado es titular de dos derechos fundamentales que hay que respetar: el derecho a su intimidad, recogido en el art. 18 de la Constitución Española, y el derecho a la protección de sus datos de carácter personal, consagrado en la Sentencia del Tribunal Constitucional 292/2000. Ambos derechos están regulados por la 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 y la LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, respectivamente.

En cuanto al objeto y ámbito de aplicación de la LOPD, señalar que la misma tiene por objeto *"garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos*

fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar" (art. 1 LOPD), siendo de aplicación *"a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"* (art. 2 LOPD).

Asimismo, el artículo 3.b) de la Ley Orgánica 15/1999 entiende por fichero *"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".* Como consecuencia de esta definición, podemos afirmar que la LOPD es aplicable tanto a los ficheros automatizados como no automatizados que contengan datos de carácter personal. En este sentido, debemos recordar que la Ley Orgánica 15/1999 es transposición de la 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, la cual establece lo siguiente con respecto a su ámbito de aplicación: *"Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"* (art. 3.1).

Ahora bien, la normativa española sobre Protección de Datos de Carácter Personal se ha caracterizado durante un gran número de años por un cierto desfase. De tal manera, la normativa de desarrollo de la antigua LEY ORGÁNICA 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal (LORTAD) fue aprobada en 1999 (siete años después de la publicación de la misma), que precisamente fue el mismo año en que apareció la Ley Orgánica 15/1999, que derogaba a la anterior. Debido a ello, se optó por mantener vigente la normativa de desarrollo de la derogada LORTAD, el REAL DECRETO 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, dándose la extraña circunstancia de que mientras la Ley Orgánica 15/1999 tenía por objeto regular tanto los tratamientos automatizados como no automatizados de datos de carácter personal, tan sólo existía desarrollo reglamentario de

medidas de seguridad para los ficheros automatizados de datos, quedando un vacío legal para la protección de los ficheros manuales o no automatizados en soporte papel que contuviesen datos de carácter personal.

Tras más de ocho años en la situación descrita, por fin se aprobó el 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, con entrada en vigor el 19 de abril de 2008, que deroga al anterior Real Decreto 994/1999 y que contempla un catálogo definitivo de medidas de seguridad aplicables tanto a los ficheros y tratamientos automatizados como no automatizados de datos de carácter personal.

Así lo viene a explicar el propio Preámbulo del Real Decreto 1720/2007:

"La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la 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, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

La nueva ley, que ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que "tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal". Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

A fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos,

1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999" (Preámbulo del Real Decreto 1720/2007, apartado I).

De tal manera, *"Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.*

Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

De tal manera, el reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados" (Preámbulo del Real Decreto 1720/2007, apartado II).

Por tanto, el Real Decreto 1720/2007 comparte ámbito objetivo de aplicación con la Ley Orgánica 15/1999: *"El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que*

los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado" (art. 2.1 Real Decreto 1720/2007).

Finalmente, el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, establece en su art. 5.c) que la Agencia de Protección de Datos colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia de la Ley Orgánica 5/1992 (entiéndase esta mención hecha ahora a la Ley Orgánica 15/1999, que derogó a la antigua LORTAD), y a tal efecto dictará instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados (entendamos ahora también no automatizados) a los principios de la Ley Orgánica. En este sentido, la Agencia Española de Protección de Datos ha dictado, desde 1995 a 2006, ocho instrucciones distintas sobre diversos aspectos concretos relacionados con la aplicación práctica de la LOPD, las cuales están disponibles en el Sitio Web de la propia AEPD.

1.1. Plazos de adecuación

1.1.1. LEY ORGÁNICA 15/1999, de 13 de diciembre

Sobre los plazos establecidos para la adecuación a la LOPD, debemos señalar que la Disposición Final Tercera de la Ley Orgánica 15/1999 establece su entrada en vigor en el plazo de un mes, contado desde su publicación en el Boletín Oficial del Estado. Dicha publicación tuvo lugar en el B.O.E. número 298, de 14 de diciembre de 1999. Ello significa que todos aquellos ficheros –automatizados o no automatizados– creados con posterioridad al 14 de enero de 2000 deben de manera inexcusable cumplir con lo establecido en la Ley Orgánica 15/1999.

Con respecto a los ficheros preexistentes a la entrada en vigor de la Ley, la Disposición Adicional Primera de la Ley Orgánica 15/1999 establece lo siguiente:

- Ficheros y tratamientos automatizados: los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. Por ende, para el caso de los ficheros y tratamientos automatizados, todos los plazos legales vencieron el pasado 14 de enero de 2003.

- Ficheros y tratamientos no automatizados: su adecuación a la Ley Orgánica 15/1999 deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados. Dicho plazo expiró el 24 de octubre de 2007.

En suma, todos los plazos legales de adecuación a la LOPD han vencido, sin excepción.

1.1.2. REAL DECRETO 1720/2007, de 21 de diciembre

En cuanto a los plazos de implantación de las medidas de seguridad recogidas en el 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, señalar que la disposición final segunda del citado Real Decreto establece su entrada en vigor a los tres meses de su íntegra publicación en el Boletín Oficial del Estado. Dicha publicación tuvo lugar en el B.O.E. número 17, de 19 de enero de 2008, entrando en vigor el 19 de abril del mismo año.

De conformidad con lo establecido en la regla tercera de la Disposición transitoria segunda del Real Decreto 1720/2007, los ficheros de datos de carácter personal, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del Real Decreto (19 de abril de 2008) deberán tener implantadas, desde el momento de su creación, la totalidad de las medidas de seguridad recogidas en el mismo.

Con respecto a los ficheros preexistentes a la entrada en vigor del Real Decreto 1720/2007 (19 de abril de 2008), ha de diferenciarse entre ficheros automatizados y no automatizados.

En primer lugar, respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del Real Decreto 1720/2007:

a) En el plazo de un año desde su entrada en vigor (el plazo finalizó el 19 de abril de 2009), deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

   1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

   2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor (el plazo finalizó el 19 de abril de 2009) deberán implantarse las medidas de seguridad de nivel medio y en el de dieciocho meses desde aquella fecha (el plazo finalizó el 19 de octubre de 2009), las de nivel alto exigibles a los siguientes ficheros:

1.º Aquéllos que contengan datos derivados de actos de violencia de género.

2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del Real Decreto 1720/2007 (el plazo finalizó el 19 de abril de 2009).

En segundo lugar, respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del Real Decreto 1720/2007:

a) Las medidas de seguridad de nivel básico deberán implantarse en el plazo de un año desde su entrada en vigor (el plazo finalizó el 19 de abril de 2009).

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor (el plazo finalizó el 19 de octubre de 2009).

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor (el plazo finalizó el 19 de abril de 2010).

2. Normativa sectorial

La LEY 14/1970, de 4 de agosto, General de Educación y Financiamiento de la Reforma Educativa (en adelante, LGE), aprobada hace más de 35 años (8 años antes de la publicación del art. 18.4 referente al derecho a la intimidad en relación con el uso de la informática en la Constitución Española de 1978, 22 años antes de la aparición de la ya derogada LORTAD, 29 años antes de la aprobación de nuestra vigente LOPD y 32 años antes de la publicación de la Sentencia del Tribunal Constitucional 292/2000 que consagró el derecho a la protección de datos como un derecho fundamental independiente), ya hacía referencia al carácter reservado de los datos del alumnado. En concreto su art. 11.3, establecía que *"De cada alumno habrá constancia escrita, con carácter reservado, de cuantos datos y observaciones sobre su nivel mental, aptitudes y aficiones, rasgos de personalidad, ambiente, familia, condiciones físicas y otras circunstancias que consideren pertinentes para su educación y orientación. Para la redacción de la misma se requerirá la colaboración de los padres. Un extracto actualizado deberá incluirse en el expediente de cada alumno al pasar de un nivel educativo a otro"*.

No obstante lo anterior, las sucesivas leyes reguladoras del Sistema Educativo español dejaron totalmente aparcada esta cuestión. De tal manera, tanto la LEY ORGÁNICA 8/1985, de 3 de julio, Reguladora del Derecho a la Educación (en adelante, LODE), como la LEY ORGÁNICA 1/1990, de 3 de octubre, de Ordenación General del Sistema Educativo (en adelante, LOGSE), no hicieron ninguna mención específica al derecho a la intimidad del alumnado. Por su parte, la LEY ORGÁNICA 10/2002, de 23 de diciembre, de Calidad de la Educación (en adelante, LOCE), mencionaba el respeto a la intimidad únicamente como un deber básico del alumnado hacia los miembros de la comunidad educativa, pero no como un derecho del propio alumnado. Asimismo, ninguna de las leyes citadas llegó a derogar el art. 11.3 de la LGE, que, pese a tener una redacción anticuada y obsoleta, continuaba vigente frente a la total ausencia de regulación de la cuestión de los datos personales del alumnado en las leyes que le sucedieron.

La inicial preocupación por los datos de carácter personal del alumnado plasmada en la Ley 14/1970 no se ha vuelto a recuperar hasta la aparición

de la LEY ORGÁNICA 2/2006, de 3 de mayo, de Educación (en adelante, LOE), que ha derogado definitivamente el citado art. 11.3, dedicando una Disposición adicional específica a los datos personales del alumnado, en consonancia con la consolidación del derecho fundamental a la protección de datos de carácter personal:

"Disposición adicional vigesimotercera. Datos personales de los alumnos.

1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.

2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos.

En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

4. La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal, y las condiciones mínimas serán acordadas por el Gobierno con las Comunidades Autónomas en el seno de la Conferencia Sectorial de Educación."

En el ámbito de nuestra Comunidad Autónoma, la LEY 17/2007, de 10 de diciembre, de Educación de Andalucía, publicada en el BOJA núm. 252,

de 26 de diciembre de 2007, contiene una disposición específica sobre los datos personales del alumnado, si bien ésta se remite directamente a lo establecido en la Disposición adicional vigesimotercera de la LOE:

"Disposición adicional segunda. Datos personales del alumnado.

En el tratamiento de los datos personales del alumnado por la Administración educativa y los centros docentes, se estará a lo dispuesto en la disposición adicional vigesimotercera de la Ley Orgánica 2/2006, de 3 de mayo."

3. Enlaces a la principal normativa sobre protección de datos de carácter personal aplicable a los centros de enseñanza

3.1. Normativa de la Unión 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. Disponible en el apartado de Protección de Datos del Sitio Web de la Comisión Europea:
  http://europa.eu/legislation_summaries/information_society/l14012_es.htm

3.2. Normativa nacional general

- LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
  http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1999-23750

- 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.
  http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2008-979

- INSTRUCCIONES dictadas por la Agencia Española de Protección de Datos en cumplimiento de lo establecido en el art. 5.c) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. Disponibles en el Canal de Documentación del Sitio Web de la Agencia Española de Protección de Datos, apartado de Legislación Estatal:
  http://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/index-ides-idphp.php

3.3. Normativa nacional y autonómica sectorial

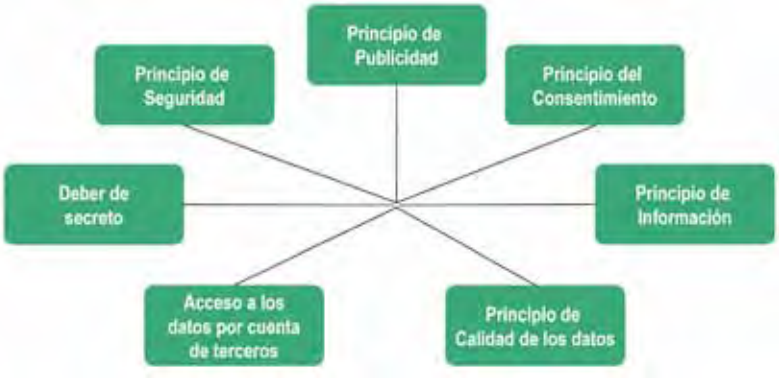
- Disposición adicional vigesimotercera de la LEY ORGÁNICA 2/2006, de 3 de mayo, de Educación.
  http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2006-7899

- Disposición adicional segunda de la LEY 17/2007, de 10 de diciembre, de Educación de Andalucía.
  http://juntadeandalucia.es/boja/boletines/2007/252/d/1.html

- Orden de 26 de abril de 2010, por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por la Consejería de Educación de la Junta de Andalucía en el ámbito de la videovigilancia en centros educativos.
  http://juntadeandalucia.es/boja/boletines/2010/91/d/20.html

CAPÍTULO III

APLICACIÓN DE LOS PRINCIPIOS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS AL ÁMBITO EDUCATIVO



1. Principio de Publicidad

El artículo 39 de la LOPD crea el Registro General de Protección de Datos (en adelante, RGPD), atribuyéndole, entre otras, la función de inscripción de los ficheros de que sean titulares las Administraciones Públicas y las entidades privadas.

Esta función del RGPD se complementa con el mandato que establece el artículo 37.j) LOPD de velar por la publicidad de la existencia de los ficheros de datos de carácter personal, a cuyo efecto publica periódicamente la relación de ficheros inscritos. Con esta información, el Registro desarrolla el principio de publicidad al facilitar a la ciudadanía el ejercicio del derecho de consulta regulado en el artículo 14 de la LOPD, informando con carácter público y gratuito, de la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del fichero (Memoria 2005 AEPD).

Por otro lado, el art. 20 LOPD se refiere expresamente a la creación, modificación o supresión de ficheros de datos de carácter personal de titularidad pública, estableciendo lo siguiente:

"Artículo 20. Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición

general publicada en el Boletín Oficial del Estado o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción."

Asimismo, el reciente Real Decreto 1720/2007, de 21 de diciembre, dedica el Capítulo I de su Título V a la *"Creación, modificación o supresión de ficheros de titularidad pública"*, estableciendo, en un sentido semejante al art. 20 LOPD, que *"La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente"* (art. 52.1) y que *"En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero*" (art. 52.2).

En cuanto a la forma que debe revestir la disposición o acuerdo de creación, modificación o supresión de los ficheros de titularidad pública, el citado Real Decreto señala lo siguiente:

"Artículo 53. Forma de la disposición o acuerdo.

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente."

Finalmente, el Real Decreto 1720/2007 reproduce, de manera casi mimética, lo establecido en el art. 20 LOPD con respecto al contenido de la disposición o acuerdo de creación, modificación o supresión de los ficheros de titularidad pública, si bien es cierto que introduce alguna leve variación que deberá ser tenida en cuenta:

"Artículo 54. Contenido de la disposición o acuerdo.

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente

protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f) Los órganos responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.

3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción."

En el caso de los centros de enseñanza pública, se plantea la duda de si ha de ser el propio centro de enseñanza o la Consejería de la cual depende quien deba proceder a la adopción de la disposición de carácter general señalada en los artículos 20 de la Ley Orgánica 15/1999 y 52 del Real Decreto 1720/2007 y la posterior publicación de la misma en el Boletín Oficial del Estado o Diario oficial correspondiente, así como a la consiguiente notificación de sus ficheros a fin de lograr su inscripción en el Registro General de Protección de Datos.

Dicha cuestión ha sido resuelta por la Agencia Española de Protección de Datos en su Informe Jurídico 143/2004, indicando lo siguiente:

"… la obligación de notificación corresponderá al responsable del fichero, definido por el artículo 3 d) de la Ley Orgánica 15/1999 como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

Para determinar a quién corresponde la obligación de proceder a la adopción de la correspondiente disposición de carácter general y la consiguiente notificación del tratamiento al Registro General del Protección de Datos resulta imprescindible delimitar si el consultante es un órgano incardinado en la Administración Autonómica o si el mismo posee personalidad jurídica independiente de la misma.

En el primer supuesto, el Centro no sería sino un mero usuario del fichero, cuyo responsable sería la Administración educativa autonómica, de forma que la obligación de notificación correspondería a la Consejería de Educación, debiendo hacerse referencia al Centro educativo únicamente como lugar de ubicación del fichero. En caso contrario, el responsable del fichero sería el propio Centro, correspondiendo al mismo la notificación del tratamiento al Registro de esta Agencia."

En este sentido, la Consejería de Educación de la Junta de Andalucía ha creado la ORDEN de 20 de julio de 2006, por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por la Consejería de Educación en el ámbito de los sistemas Séneca y Pasen, publicada en el BOJA núm. 156, de fecha 11 de agosto de 2006.

2. Principio del Consentimiento

2.1. Características del consentimiento

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, consagró el derecho a la protección de datos de carácter personal como un derecho fundamental independiente, desvinculado del derecho a la intimidad, cuyo contenido está integrado por los principios y derechos que se contemplan en la LOPD.

Este derecho autónomo e informador de nuestro texto constitucional se concreta en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a su posesión o uso.

Como consecuencia de lo anterior, todo tratamiento de datos de carácter personal requiere el consentimiento previo e inequívoco del interesado, interesada o titular de los mismos, principio legitimador en torno al cual se vertebra la normativa española sobre protección de datos y que permite a la persona ejercer el control efectivo del uso de sus datos por parte de terceros.

A este respecto, la Ley Orgánica de Protección de Datos de Carácter Personal define el consentimiento del interesado como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen"* (art. 3.h). El nuevo Real Decreto 1720/2007 recoge idéntica definición del consentimiento en su art. 5.1.d).

De ello se desprende que para que el consentimiento pueda ser considerado conforme a Derecho deben concurrir necesariamente los cuatro requisitos enumerados.

A juicio de la Agencia Española de Protección de Datos la interpretación

que ha de darse a estas cuatro notas características del consentimiento ha de ser la siguiente:

- ***Libre***

Esto supone que el consentimiento deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil (por ejemplo, violencia o intimidación).

- ***Específico***

Es decir, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.1 de la Ley Orgánica de Protección de Datos de Carácter Personal.

- ***Informado***

Esto es, que el afectado o afectada conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce.

En este sentido, el consentimiento del o la titular de los datos deberá ir, en todo caso, precedido de una declaración del Responsable del Fichero en la que se informe de manera clara y precisa de la inclusión de sus datos en un fichero, de los usos que se prevé dar a los mismos, de los posibles destinatarios de los datos, etc., a fin de que aquel o aquella consienta o no a dar sus datos siendo plenamente consciente de a quién y para qué los está facilitando.

- ***Inequívoco***

Esto implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado o afectada (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

En interpretación de la Agencia Española de Protección de Datos, de las características del consentimiento no se infiere necesariamente su carácter expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter, lo ha indicado expresamente; así sucede en el caso de tratamiento de datos especialmente protegidos indicando el artículo 7.2 de la Ley Orgánica de Protección de Datos la necesidad de consentimiento expreso y escrito para el tratamiento de los datos de ideología, religión, creencias y afiliación sindical, y el artículo 7.3 la necesidad de consentimiento expreso aunque no necesariamente escrito para el tratamiento de los datos relacionados con la salud, el origen racial y la vida sexual. Sobre ello trataremos en el apartado siguiente.

Por tanto, el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos, si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado o afectada un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo.

Por otro lado, el 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, hace referencia a los *"Principios generales"* del consentimiento, realizando una serie de precisiones que habrán de ser observadas a la hora de solicitar el consentimiento del interesado para el tratamiento de sus datos de carácter personal:

- El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes (art. 12.1, párrafo primero).

- La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones

que concurran en el tratamiento o serie de tratamientos (art. 12.1, párrafo segundo).

- Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo (art. 12.2).

- Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho (art. 12.3). Esto es, lo que jurídicamente se denomina *"carga de la prueba"* recae, conforme a lo establecido en el Real Decreto 1720/2007, sobre el responsable del tratamiento.

2.2. Datos Especialmente Protegidos

El art. 7 de la Ley Orgánica 15/1999, configura bajo la rúbrica general de *"Datos especialmente protegidos"*, un régimen especialmente cualificado, con protección más intensa, para aquellos datos personales que proporcionan una información de esferas íntimas del individuo (Sentencia de la Audiencia Nacional de fecha 12 de abril de 2002, recurso 1271/2000).

De tal manera, el art. 7.2 LOPD establece que *"Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias"*.

Asimismo, *"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente"* (art. 7.3 LOPD).

Algunos ejemplos habituales de datos especialmente protegidos que pueden ser tratados en los centros de enseñanza son los siguientes:

- Los datos psicológicos contenidos en los informes psicopedagógicos, test de inteligencia y conducta, etc. confeccionados por los orientadores y orientadoras (datos referentes a la salud del alumnado).

- El dato del grado de minusvalía de determinados alumnos y alumnas con necesidades educativas especiales.

- Los datos sobre alergias a determinados alimentos de algunos alumnos y alumnas, para su conocimiento por parte del servicio de comedor escolar.

- Los datos referentes a determinados alumnos y alumnas que presenten problemas de salud que les imposibilite el ejercicio físico.

- El dato del origen racial de algunos alumnos y alumnas.

Sin embargo, el dato relacionado con el hecho de que el alumno o la alumna curse o no la asignatura de religión no tiene la consideración de dato especialmente protegido, ya que, en interpretación de la Agencia Española de Protección de Datos*, "el hecho mismo de cursar la asignatura de religión no revela necesariamente que el estudiante profese las creencias a las que tal asignatura se refiere, del mismo modo que el hecho de no cursarla no revela la inexistencia de esas creencias, sino que tal circunstancia puede deberse al estudio de la religión en otros foros distintos del escolar. Es decir, a nuestro juicio, lo único que revela el dato de optar por cursar la asignatura de religión sería el interés del alumno por conocer los principios, historia y preceptos de la misma, sin que ello implique una efectiva confesionalidad del mismo, a cuya declaración no podría encontrarse obligado".*

2.3. Consentimiento otorgado por personas menores de edad

En el ámbito educativo la cuestión del consentimiento se complica, ya que en la gran mayoría de los casos estamos hablando de personas menores de edad. Surge, por tanto, la inevitable pregunta de si éstas gozan

o no de la capacidad jurídica suficiente para consentir sobre el tratamiento de sus datos.

Nuestra Ley Orgánica de Protección de Datos no hace referencia a esta cuestión. Dicha falta de previsión legislativa ha provocado que en diversas ocasiones se haya planteado ante la Agencia Española de Protección de Datos qué requisitos debería reunir el consentimiento otorgado por los y las menores de edad para el tratamiento de sus datos, cuestión que la misma resolvió en su Memoria 2000.

En la citada Memoria, la AEPD determinó que, con carácter general, deben diferenciarse dos supuestos básicos: el primero referido a los y las mayores de catorce años, a los/las que la Ley atribuye capacidad para la realización de determinados negocios jurídicos, y el consentimiento que pudieran dar los y las menores de dicha edad. Partiendo de esta premisa, la Agencia Española de Protección de Datos elaboró la siguiente argumentación:

"Respecto de los mayores de catorce años, debe recordarse en primer término, que el artículo 162.1º del Código Civil exceptúa de la representación legal del titular de la patria potestad a "los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo".

Se plantea entonces si, en el supuesto de mayores de catorce años, ha de considerarse que el menor tiene condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos, debiendo, a nuestro juicio, ser afirmativa la respuesta, toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil. Baste a estos efectos recordar los supuestos de adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, que se efectuará por el mayor de catorce años, asistido de su representante legal, o la capacidad para testar (con la única excepción del testamento ológrafo) prevista en el artículo 662.1 del Código Civil para los mayores de catorce años.

Por otra parte, debe recordarse que, según tiene señalado la Dirección General de Registros y del Notariado, en resolución de 3 de marzo de 1989, "no existe una norma que, de modo expreso, declare su incapacidad para actuar válidamente en el orden civil, norma respecto de la cual habrían de considerarse como excepcionales todas las hipótesis en que se autorizase a aquél para obrar por sí; y no cabe derivar esa incapacidad ni del artículo 322 del Código Civil, en el que se establece el límite de edad a partir del cual se es capaz para todos los actos de la vida civil, ni tampoco de la representación legal que corresponde a los padres o tutores respecto de los hijos menores no emancipados". En resumen, la minoría de edad no supone una causa de incapacitación (de las reguladas en el artículo 200 del Código Civil), por lo que aquélla habrá de ser analizada en cada caso concreto a los efectos de calificar la suficiencia en la prestación del consentimiento en atención a la trascendencia del acto de disposición y a la madurez del disponente.

A mayor abundamiento, y en lo referente a la prestación del consentimiento para la cesión, debe recordarse que, conforme dispone el artículo 4.3 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, "se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales". Del tenor de esta disposición se deriva la posibilidad de que haya sido el propio menor quien, por sí mismo, haya prestado su consentimiento a la utilización de su propia imagen, sin precisar para ello la asistencia de su representante legal, lo que no hace sino ahondar en la conclusión ya referida anteriormente, a partir de lo dispuesto en el artículo 162 del Código Civil.

En consecuencia, a tenor de las normas referidas, cabe considerar que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismo, el tratamiento automatizado de sus datos de carácter personal."

En suma, en base a la interpretación que la Agencia Española de Protección de Datos ha realizado del art. 162.1º del Código Civil en conjunción

con otra serie de normas, cabe considerar que, con carácter general, los y las mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismos/as, el tratamiento automatizado (y, por tanto, no automatizado) de sus datos de carácter personal.

Respecto de los y las restantes menores de edad, la AEPD señala que *"no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162.1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez.*

En consecuencia, a la vista de lo anteriormente señalado, será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley, recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales."

Con respecto a los y las menores de catorce años que no reúnan las condiciones de madurez suficientes para consentir sobre el tratamiento de sus datos pueden surgir, adicionalmente, otra serie de cuestiones. Por ejemplo, ¿qué ocurriría en el caso de los padres separados? ¿Quién ostentaría en dicho supuesto la representación legal del o la menor para el tratamiento de sus datos? Dicha cuestión ha sido tratada por la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), la cual ha señalado que *"en los casos de padres separados, como señala el artículo 162 del Código Civil, los padres que ostenten la patria potestad tienen la representación legal de sus hijos menores no emancipados. La resolución judicial de la separación es la que establece lo relativo a la patria potestad y a la guardia y custodia de los hijos, siendo normalmente compartida la primera, y asignada la segunda a uno de los progenitores. El ejercicio de la patria potestad es determinante para ostentar el ejercicio de la representación legal de los menores..."*.

De lo anterior se desprende que, en el caso de unos padres separados, ambos progenitores ostentarían la representación legal del o la menor para el tratamiento de sus datos, salvo en el caso concreto de que alguno de ellos estuviese privado judicialmente de la patria potestad del hijo o hija menor, en cuyo caso la privación de la patria potestad implicaría su pérdida de la condición de representante legal, inclusive, como es lógico, para consentir sobre el tratamiento de los datos de carácter personal del o la menor.

El reciente 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 incorpora, de manera definitiva, el criterio interpretativo de la Agencia Española de Protección de Datos plasmado en su Memoria 2000, regulando, asimismo, otros aspectos de importancia en referencia a la captación de datos de menores:

"Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales."

De tal manera, el apartado 1 del citado artículo 13 sitúa definitivamente la barrera del consentimiento para el tratamiento de los datos de las personas menores de edad en los catorce años, señalando que *"podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela"* y que *"en el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores"*.

A partir de este presupuesto teórico surge una rica casuística. Este es, por ejemplo, el caso del tratamiento de los datos de salud de la persona menor de edad en relación con la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (en adelante, LAP). La Ley de Autonomía del Paciente, dentro de sus principios básicos, establece que *"Toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento, que debe obtenerse después de que el paciente reciba una información adecuada, se hará por escrito en los supuestos previstos en la Ley"* (art. 2.2 LAP).

Con respecto a las personas menores de edad, la Ley 41/2002 establece que *"Se otorgará el consentimiento por representación cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor después de haber escuchado su opinión si tiene doce años cumplidos. Cuando se trate de menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, no cabe prestar el consentimiento por representación. Sin embargo, en caso de actuación de grave riesgo, según el criterio del facultativo, los padres serán informados y su opinión será tenida en cuenta para la toma de la decisión correspondiente"* (art. 9.3.c) LAP).

Por tanto, cualquier actuación en el ámbito de la salud de los pacientes menores de edad requerirá el consentimiento de sus representantes legales, salvo en el caso de que tenga los dieciséis años cumplidos y no haya sido declarado incapaz. De tal manera, parece que, en principio, el criterio aplicable debería ser el recogido en la Ley de Autonomía del Paciente (dieciséis años) y no el contemplado en el artículo 13 del Real Decreto 1720/2007 (catorce años), ya que es a partir de los dieciséis años cuando se entiende que el menor dispone de las condiciones de madurez suficientes para consentir sobre cualquier actuación en el ámbito de su salud y sobre el tratamiento de sus datos de carácter personal de manera conjunta.

De igual manera, el menor o la menor que padezca una enfermedad o deficiencia persistente de carácter físico o psíquico que le impida gobernarse por sí mismo o por sí misma podrá ser declarado o declarada incapaz por sentencia judicial, tal y como establecen los artículos 199 a 201 del Código Civil español, en cuyo caso necesitaría el complemento de la capacidad de los titulares de la patria potestad o tutela para poder consentir sobre el tratamiento de sus datos de carácter personal, con total independencia de si ha cumplido o no los catorce años de edad:

"Artículo 199.

Nadie puede ser declarado incapaz sino por sentencia judicial en virtud de las causas establecidas en la Ley.

Artículo 200.

Son causas de incapacitación las enfermedades o deficiencias persistentes de carácter físico o psíquico que impidan a la persona gobernarse por sí misma.

Artículo 201.

Los menores de edad podrán ser incapacitados cuando concurra en ellos causa de incapacitación y se prevea razonablemente que la misma persistirá después de la mayoría de edad."

Por otro lado, según lo establecido en nuestra Ley Orgánica 15/1999, los datos de las personas menores de edad no tienen la consideración de *datos especialmente protegidos* como tal, categoría reservada, en un principio, a los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, los que hagan referencia al origen racial o étnico, a la salud y a la vida sexual y los relativos a la comisión de infracciones penales o administrativas. El Borrador de Reglamento de desarrollo de la Ley Orgánica 15/1999 llegó a contemplar, en su versión de fecha 24 de octubre de 2005, la inclusión de los datos de las personas menores de catorce años dentro de la categoría de datos de nivel medio, si bien dicha posibilidad fue rehusada con el paso del tiempo. Ahora bien, ello no significa que los datos de los menores no pertenezcan a una categoría *sui generis* que podríamos llamar *datos de personas especialmente vulnerables*, basada en un criterio subjetivo en función de la persona titular de los datos y las especiales condiciones que le rodean.

Pensemos en lo valioso que puede ser para una empresa con una política comercial agresiva el incorporar a sus ficheros los datos de un menor al cual poder bombardear durante el resto de su vida con ofertas y promociones perfectamente adecuadas a su perfil de consumo, seguido con detenimiento desde su infancia. En este sentido, GISBERT JORDÁ señala, con gran dosis de acierto, que *"el sector infantil y juvenil constituye un punto de creciente atención en los últimos años por parte del marketing comercial que lo considera un mercado de gran potencial en expansión"*.

Esta situación se ha visto agravada con la irrupción de las nuevas Tecnologías de la Información y las Comunicaciones (cada día que pasa menos nuevas y más familiares para todos, especialmente para niños y adolescentes), conocidas bajo el acrónimo TICs y representadas no solamente por Internet (entendido éste en su sentido tradicional) sino también por otro tipo de tecnologías emergentes como, por ejemplo, los teléfonos móviles de última generación. Estas nuevas tecnologías configuran un nuevo espacio universal y anárquico donde el menor facilita sus datos de carácter personal de manera inconsciente, despreocupada y casi compulsiva a una multitud de terceros desconocidos sin control alguno.

En efecto, el menor proporciona a lo largo de su infancia y adolescencia sus datos de carácter personal de manera descontrolada a una multitud de empresas, entidades y organizaciones sin llegar a ser realmente consciente de que ello pueda afectar a su propia intimidad e incluso a la de su familia. En la inmensa mayoría de los casos, el menor no sólo ignora por completo su derecho a la protección de sus datos de carácter personal y lo que ello significa, sino que además tampoco se siente especialmente preocupado o molesto a la hora de tener que facilitar sus datos a terceros, como puede suceder en el caso de los adultos, haciéndolo gustoso si a cambio existe la promesa de un atractivo regalo.

Por otro lado, el desconocimiento del menor es el instrumento perfecto para obtener a través de él aquellos datos de sus familiares (padres, hermanos mayores, etc.) que en circunstancias normales un adulto probablemente se hubiese negado a facilitar (por ejemplo, datos acerca de la situación económica de la familia o de la ideología, religión o creencias de sus padres).

Todo lo anterior justifica, como puede entenderse, la introducción del apartado segundo del artículo 13 en el nuevo Real Decreto 1720/2007: *"en ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior"*.

En tercer lugar, el citado artículo 13 establece que *"cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo"* (apartado 3).

De tal manera, la redacción del texto para cumplir con el deber de información conforme a lo establecido en nuestra normativa sobre

protección de datos de carácter personal no debería ser la misma en el caso de que dicha información vaya dirigida a un menor que cuando esté orientada hacia una persona adulta. Esta reflexión adquiere una mayor trascendencia debido a la ausencia de un asentamiento firme de una cultura de la protección de datos en nuestra sociedad (al contrario, por ejemplo, que la cultura de la educación vial que sí está mucho más asentada, llegando a estudiarse algunas nociones básicas en los colegios), lo que origina que, en la inmensa mayoría de los casos, el menor ignore por completo lo que significa el derecho a la protección de sus datos de carácter personal.

En virtud de lo anterior, se antoja indispensable que cuando se informe al menor de los extremos contemplados en el artículo 5 de la Ley Orgánica 15/1999 se haga en un lenguaje sencillo y fácilmente comprensible, carente de conceptos jurídicos abstrusos. De lo contrario, el menor carecería de poder de disposición y control alguno sobre sus propios datos de carácter personal, escaparían a su control porque simplemente no se le está explicando qué utilización se va a hacer de sus datos de manera que él lo entienda.

Finalmente, el apartado 4 del artículo 13 del Real Decreto 1720/2007 señala que *"corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales"*.

Este apartado debe enlazarse con el artículo 12 apartado 3 del Real Decreto 1720/2007, que establece que *"corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho"* y con el artículo 18 de la misma norma, relativo a la *"Acreditación del cumplimiento del deber de información"*:

"Artículo 18. Acreditación del cumplimiento del deber de información.

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales."

Poniendo en común las disposiciones legales citadas, corresponde al responsable del fichero o tratamiento el cumplimiento de las siguientes obligaciones:

- Articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales. En este sentido, corresponderá al responsable del fichero o tratamiento la prueba de la existencia del consentimiento del afectado –o, en su caso, de sus padres, tutores o representantes legales– por cualquier medio de prueba admisible en derecho.

- Utilizar un medio que permita acreditar el cumplimiento del deber de información, debiendo conservarse el soporte en el que conste mientras persista el tratamiento de los datos del afectado.

El cumplimiento de las citadas obligaciones puede ser una tarea relativamente sencilla si se solicita el consentimiento informado por escrito (por ejemplo, a través del Formulario de Matriculación), de tal manera que el padre, madre, tutor o representante legal otorgue a través de su firma manuscrita el consentimiento para el tratamiento de los datos de su hijo o hija menor de catorce años.

Ahora bien, la cuestión de la obtención de un consentimiento válido para el tratamiento de los datos del o la menor se complica hasta extremos insospechados en el ámbito de las anteriormente citadas Tecnologías de la Información y las Comunicaciones, debido a las características intrínsecas del mundo digital que todos tenemos en mente.

En primer lugar, existe un problema serio con respecto al cumplimiento del principio de calidad de los datos establecido en el art. 4 LOPD, ya que es muy complicado garantizar la exactitud y veracidad de los datos aportados por el o la menor. En este sentido, podría darse perfectamente el caso de que el o la menor no facilitase sus propios datos, sino los de un amigo, un compañero de clase o alguno de sus hermanos. O bien que manifestase haber superado la barrera de los catorce años de edad establecida en el Real Decreto 1720/2007 para consentir sobre el tratamiento de sus datos sin ser ello cierto. El problema es, en todo caso, cómo constatarlo.

La complicada cuestión de la obtención del consentimiento para el tratamiento de los datos del menor en el ámbito de las TICs ha sido obviada hasta la fecha por nuestro ordenamiento jurídico. Sin embargo, sí que ha sido abordada desde hace unos cuantos años y con bastante acierto en el ámbito de los Estados Unidos, donde se han estableciendo una serie de mecanismos para la obtención del consentimiento, cuya complejidad y rigurosidad aumenta de manera gradual en función de los riesgos que para la intimidad del menor puedan tener los diferentes tratamientos y usos que se vayan a hacer de sus datos de carácter personal. Algunos de los métodos contemplados en Estados Unidos en orden a la obtención del consentimiento del padre, madre, tutor o representante legal del menor para el tratamiento de sus datos son los siguientes: un escrito firmado por el padre o representante legal del menor y enviado por medio de correo postal ordinario o a través de fax, una llamada telefónica del padre o representante legal del menor o un mensaje de correo electrónico firmado digitalmente por el padre o representante legal del menor.

2.4. Limitaciones al principio del consentimiento en los centros de enseñanza públicos

El derecho a la protección de datos de la ciudadanía tiene contenidos distintos cuando se trata de ficheros privados (por ejemplo, el fichero de clientes de una empresa privada) o a tratamientos en ficheros públicos (por ejemplo, el fichero de alumnos y alumnas de un centro de enseñanza de carácter público). Así, mientras que el responsable del fichero privado

sólo puede alegar en la mayoría de las ocasiones una legítima actividad de negocio protegida por la libertad de empresa (art. 38 Constitución Española), el titular de un fichero público procede a tratamientos de datos de carácter personal para desarrollar la efectividad de derechos fundamentales reconocidos en la Constitución, en nuestro caso la actividad prestacional de educación prevista en el art. 27 Constitución Española.

De tal manera, el derecho a la protección de datos de carácter personal del alumnado se ve afectado por ciertas limitaciones cuando lo que está en juego es garantizar la efectividad del derecho fundamental a la educación por parte de los poderes públicos. En concreto, la Ley Orgánica 15/1999 establece en su art. 6.2 que no será preciso el consentimiento del afectado o afectada (en nuestro caso, el alumno, la alumna o su padre, madre o representante legal si no reúne las condiciones de madurez suficientes) para la recogida y tratamiento de sus datos de carácter personal cuando los mismos se recaben para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias (la actividad prestacional de educación en el caso de un centro educativo público).

Asimismo, la Disposición adicional vigesimotercera de la LOE establece que *"la incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad"*. Por tanto, el mero hecho de la incorporación del alumno o la alumna al centro educativo comporta, en principio, el consentimiento para el tratamiento de sus datos.

En cualquier caso, la excepción al principio del consentimiento que plantea la Disposición adicional vigesimotercera de la LOE queda limitada exclusivamente a la *"función docente y orientadora"* del centro, no pudiendo tratarse los datos del alumnado con fines diferentes del educativo sin el consentimiento expreso de los mismos/as o de sus padres, madres o representantes legales, según proceda.

Asimismo, el art. 21.1 LOPD establece que *"Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas*

para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos". Dicho precepto, interpretado a *sensu contrario*, significa que está habilitada la comunicación de datos entre Administraciones Públicas para el ejercicio de competencias idénticas o que versen sobre las mismas materias (por ejemplo, Ministerio de Educación y Consejería de Educación), lo cual supone una nueva excepción al principio del consentimiento. Ahora bien, habrá que atender a las condiciones particulares de cada cesión de datos entre Administraciones Públicas para ver si sería de aplicación la citada excepción.

Por otra parte, el 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, hace referencia en su artículo 10 a los supuestos que legitiman el tratamiento o cesión de los datos, señalando, en primer lugar, que los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado *"cuando se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario"* (art. 10.3.a). Con respecto a la cesión de datos de carácter personal entre Administraciones Públicas sin contar con el consentimiento del interesado, el art. 10.4.c) del citado Real Decreto establece que ésta será posible cuando concurra uno de los siguientes supuestos:

- Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

- Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

- La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

3. Principio de Información

3.1. Características del derecho de información

Tal y como señala la propia Agencia Española de Protección de Datos, el deber de información al afectado, previo al tratamiento de sus datos de carácter personal, es uno de los principios fundamentales sobre los que se asienta la Ley Orgánica 15/1999 y así viene incluido dentro de su Título II.

En este sentido, la trascendental Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, ha señalado lo siguiente*: "son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.*

Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele" (Fundamento Jurídico 7).

En concreto, el derecho de información queda recogido en el art. 5 de la Ley Orgánica 15/1999, el cual señala lo siguiente:

"Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

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

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

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

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b, c y d del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a, d y e del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada

comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten."

La Sala de lo Contencioso-Administrativo de la Audiencia Nacional, en su Sentencia de 15 de junio de 2001, también ha profundizado en el derecho de información establecido en el art. 5 LOPD, señalando lo siguiente: *"En primer lugar, debe tenerse en cuenta que nos hallamos ante la regulación del derecho de la información a la recogida de datos, derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos y así lo valora el texto positivo al pormenorizar su contenido y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco. La relevancia del derecho conlleva que su exclusión requiera el mandato expreso de una norma, acogiendo una interpretación estricta, vedándose su extensión mediante artificiosas deducciones"*.

De tal manera, conforme a lo establecido en el art. 5 LOPD, el alumno, la alumna o su padre, madre o representante legal, cuando así proceda, deben ser escrupulosamente informados con carácter previo a la recogida de sus datos (ya sea a través de los formularios de solicitud de plaza y matriculación, de la ficha que el profesorado utiliza para el control de sus alumnos y alumnas o a través de cualquier otro canal de recogida) de la finalidad para la que éstos se recogen, de los destinatarios de la información que faciliten, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, así como de la identidad y dirección del responsable del tratamiento.

La Consejería de Educación de la Junta de Andalucía, consciente del deber de información recogido en la Ley Orgánica 15/1999, ha diseñado una serie de modelos orientativos de cláusulas legales a incorporar en los impresos y formularios de uso frecuente de los centros de enseñanza de la Junta de Andalucía para la recogida de datos de carácter personal, en cumplimiento de lo establecido en el art. 5 LOPD.

Recordar, por último, que el tantas veces citado Real Decreto 1720/2007 también dedica un artículo específico al deber de información, sobre el que ya hemos tratado en el apartado relativo al principio del consentimiento y que, por tanto, nos limitamos a reproducir nuevamente:

"Artículo 18. Acreditación del cumplimiento del deber de información.

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales."

4. Principio de calidad de los datos

El principio de calidad de los datos es otro de los pilares sobre los que se asienta la normativa española sobre protección de datos de carácter personal. Viene regulado en el Título II de la LOPD, más concretamente en su art. 4, que establece lo siguiente:

"Artículo 4. Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos."

De lo aquí transcrito, podemos afirmar que las obligaciones contenidas en el art. 4 LOPD se condensan en las siguientes:

- Obligación de que los datos sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente. Esto es, no deben recogerse datos de carácter personal más allá de los estrictamente necesarios para atender a la finalidad concreta para la cual se solicitan.

  Por citar un caso, no tendría sentido que un centro de enseñanza solicitase el dato de confesión religiosa de los padres y madres para tramitar la solicitud de plaza o la matriculación de los futuros alumnos y alumnas, teniendo la consideración de dato excesivo.

  Por otro lado, el informe 368/06 de la Agencia Española de Protección de Datos se refiere a la conformidad con la LOPD de la creación de un sistema de control para gestionar las ausencias y retrasos de los alumnos de un centro escolar mediante la obtención de su huella dactilar, por la que se controlaría la entrada y salida de los alumnos de dicho centro. A tal efecto, se considera que el tratamiento del dato biométrico de la huella digital para las finalidades señaladas puede resultar contrario al principio de proporcionalidad en el tratamiento, consagrado por el artículo 4.1 de la LOPD, teniendo en cuenta los precedentes contenidos en el Documento de Trabajo sobre biometría, aprobado por el Grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE, de fecha 1 agosto de 2003, referentes a decisiones adoptadas en este sentido por las autoridades de protección de datos de Francia y Portugal.

- Obligación de respetar la finalidad concreta para la cual han sido recogidos los datos de carácter personal. Por ejemplo, no tendría sentido que los datos recabados en la solicitud de plaza de un alumno o alumna sean utilizados para ofrecerle información sobre una colección literaria específicamente destinada al público infantil y juvenil.

- Obligación de actualizar los datos y rectificarlos cuando fueran inexactos. En este sentido, constituye infracción de carácter grave, de acuerdo con lo dispuesto en el artículo 44.3.f) LOPD, *"Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara".*

- Obligación de cancelar los datos, sin necesidad de solicitud previa del afectado o afectada, cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados.

- Obligación de cumplir con unos determinados deberes éticos en la recogida de datos de carácter personal. A este respecto, el art. 44.4.a) LOPD establece que constituye una infracción muy grave *"La recogida de datos en forma engañosa y fraudulenta"*.

El 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, reproduce, en gran medida, lo establecido en el artículo 4 de la LOPD, si bien adiciona algunas precisiones referentes a aspectos formales sobre la actualización y puesta al día de los datos, así como la cancelación de los mismos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados:

"Artículo 8. Principios relativos a la calidad de los datos.

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación."

5. Acceso a los datos por cuenta de terceros

En ciertas ocasiones, los centros de enseñanza recurren a los servicios de terceras empresas o profesionales para cubrir determinadas necesidades. Pues bien, esta cuestión adquiere una especial trascendencia cuando, para la prestación del servicio solicitado, esa tercera empresa o profesional necesita tener acceso a los datos de carácter personal gestionados en el centro (por ejemplo, datos del alumnado).

En este sentido, el art. 12.1 de la Ley Orgánica 15/1999 establece expresamente que *"no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento"*.

Ese tercero prestador del servicio es lo que la LOPD denomina *"encargado del tratamiento"*, esto es, *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento"* (art. 3.g) LOPD). Entre los ejemplos más habituales de encargados del tratamiento en el ámbito de los centros de enseñanza, podemos citar los siguientes:

- La empresa prestadora del servicio de comedor escolar, a la cual le puede ser proporcionado el listado de alumnos y alumnas apuntados al mismo, incluyendo posibles alergias a determinados alimentos.

- La empresa prestadora del servicio de transporte escolar, a la cual se facilitan los datos de aquellos alumnos y alumnas que han solicitado el mismo.

- Las terceras empresas encargadas del desarrollo e impartición de las actividades extraescolares del centro de enseñanza.

- Terceras empresas prestadoras de servicios de grabación de datos, a las cuales se faciliten formularios donde puedan constar datos de carácter personal del alumnado del centro de enseñanza (solicitudes de plaza, matriculación, solicitudes de becas, etc.).

- Terceras empresas a las cuales se encomiende la recogida y posterior destrucción de toda la documentación en soporte papel inservible almacenada en el centro de enseñanza.

- El laboratorio fotográfico al cual se le facilitan el nombre y apellidos del alumnado del centro de enseñanza para confeccionar las orlas académicas.

Aunque, como hemos indicado, estos son sólo algunos ejemplos de un largo etcétera, pudiendo darse otros muchos supuestos de encargados de tratamiento en la casuística particular de cada centro de enseñanza.

Asimismo, la propia Ley Orgánica 15/1999 impone en su art. 12 una serie de obligaciones, con la finalidad de asegurar que el tratamiento de datos realizado por la tercera empresa o profesional para la prestación del servicio cumpla con los principios y garantías establecidos en la misma:

"Artículo 12. Acceso a los datos por cuenta de terceros.

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a

otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente."

De tal manera, la relación entre el responsable del fichero y el encargado del tratamiento deberá regularse contractualmente conforme a lo dispuesto en el art. 12 LOPD, siendo de destacar, a juicio de la Agencia Española de Protección de Datos, las siguientes cuestiones:

"a) En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 impone que "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".

b) Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece que "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

c) En lo referente a la cesión de los datos, de lo establecido en el artículo 12.2 se desprende que no procederá esa cesión, de forma que los datos habrán de ser entregados única y exclusivamente al responsable del fichero.

d) En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica.

e) *Por último, según el artículo 12.4, "en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente", siendo, en consecuencia, de aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la Ley, sujetando el primero de ellos al encargado del tratamiento a dicho régimen."*

En el caso de los centros públicos de la Junta de Andalucía, el responsable de los ficheros es, en principio, la Secretaría General Técnica de la Consejería de Educación (ver Capítulo III, apartado 1 de la presente Guía).

El alcance del artículo 12 de la Ley Orgánica 15/1999 tiene reflejo en la propia Disposición adicional trigésimo primera de la LEY 30/2007, de 30 de octubre, de Contratos del Sector Público, que lleva por rúbrica *"Protección de datos de carácter personal"*. La citada Ley tiene por objeto *"regular la contratación del sector público, a fin de garantizar que la misma se ajusta a los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos, y no discriminación e igualdad de trato entre los candidatos, y de asegurar, en conexión con el objetivo de estabilidad presupuestaria y control del gasto, una eficiente utilización de los fondos destinados a la realización de obras, la adquisición de bienes y la contratación de servicios mediante la exigencia de la definición previa de las necesidades a satisfacer, la salvaguarda de la libre competencia y la selección de la oferta económicamente más ventajosa"*. Es igualmente objeto de la Ley 30/2007 *"la regulación del régimen jurídico aplicable a los efectos, cumplimiento y extinción de los contratos administrativos, en atención a los fines institucionales de carácter público que a través de los mismos se tratan de realizar".*

De tal manera, la Disposición adicional trigésimo primera de la Ley 30/2007 establece lo siguiente:

"Disposición adicional trigésimo primera. Protección de datos de carácter personal.

1. Los contratos regulados en la presente Ley que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo.

2. Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento.

En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre. En todo caso, las previsiones del artículo 12.2 de dicha Ley deberán de constar por escrito.

Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que ésta hubiese designado.

El tercero encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

3. En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:

a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.

b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.

c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos, el tercero tendrá también la consideración de encargado del tratamiento."

Por otro lado, el 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, profundiza en la figura del encargado del tratamiento y en sus relaciones con el responsable del fichero o tratamiento, realizando algunas matizaciones respecto a lo establecido en el artículo 12 de la Ley Orgánica 15/1999:

"Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo."

Asimismo, el Real Decreto 1720/2007 incorpora una importante novedad que también ha sido recogida en la anteriormente citada Ley 30/2007, de 30 de octubre, de Contratos del Sector Público: la habilitación al encargado del tratamiento para poder subcontratar los servicios con un tercero, posibilidad en principio no contemplada en la Ley Orgánica 15/1999, ya que cualquier transmisión de los datos a un tercero que no sea propiamente el responsable del fichero es considerada cesión y, en base a lo establecido en el art. 12.2 LOPD, el encargado del tratamiento no puede comunicar los datos, ni siquiera para su conservación, a terceros. Ahora bien, dicha

subcontratación de servicios debe estar sujeta, de manera inexcusable, a una serie de requisitos que se recogen en el art. 21 del citado Real Decreto:

"Artículo 21. Posibilidad de subcontratación de los servicios.

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.
Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.
En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior."

De otro lado, el artículo 22 del nuevo Real Decreto realiza algunas precisiones con respecto a la conservación de los datos por el encargado del tratamiento. Como hemos señalado anteriormente, el artículo 12.3 de la LOPD establece que *"una vez cumplida la prestación contractual, los datos*

de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento", si bien el Real Decreto 1720/2007 impone al encargado del tratamiento la obligación de conservar dichos datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento:

"Artículo 22. Conservación de los datos por el encargado del tratamiento.

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento."

Con respecto al cumplimiento de las medidas de seguridad en el tratamiento de datos de carácter personal, el nuevo Real Decreto 1720/2007 realiza una triple distinción:

1. Que el acceso del encargado del tratamiento a los datos de carácter personal se realice en los locales del responsable del fichero o del tratamiento.

2. Que el acceso del encargado del tratamiento a los datos de carácter personal sea remoto, habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable del fichero o del tratamiento.

3. Que el tratamiento de datos de carácter personal consecuencia de la relación de prestación de servicios sea realizado en los propios locales del encargado del tratamiento, ajenos a los del responsable del fichero o del tratamiento.

De tal manera, el Real Decreto 1720/2007 establece que *"cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento"* (art. 82.1 párrafo primero).

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, *"este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento"* (art. 82.1 párrafo segundo).

En tercer lugar, si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, de conformidad con lo establecido en el art. 82.2 del Real Decreto 1720/2007, deberá elaborar un documento de seguridad en los términos exigidos en su artículo 88 o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

Finalmente el art. 82.3 señala que en todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en el Real Decreto 1720/2007.

En aquellos supuestos en que la prestación de servicios no conlleve el tratamiento de datos de carácter personal, el contrato de prestación de servicios deberá, de conformidad con lo establecido en el art. 83 párrafo segundo del Real Decreto 1720/2007, recoger expresamente la prohibición del personal ajeno de acceder a los datos personales y la obligación de secreto respecto a los datos que hubiera podido conocer con motivo de la prestación del servicio. Este podría ser el caso de las empresas prestadoras

de servicios de limpieza, cuya prestación no implica el tratamiento de datos de carácter personal, pero que, sin embargo, tienen acceso a las dependencias del centro de enseñanza, donde se almacenan los datos de carácter personal del alumnado, personal docente, etc.

6. Deber de Secreto

La Disposición adicional vigesimotercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, establece que *"el profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo"*.

En este sentido, el art. 10 LOPD, bajo la rúbrica de *"Deber de secreto"*, determina que *"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*.

Esto es, la Ley Orgánica 15/1999 establece en su art. 10 un deber de secreto para todo aquél o aquélla que tenga acceso a los datos de carácter personal gestionados en el centro en el desempeño de sus funciones (por ejemplo, el o la docente que accede al programa de gestión del alumnado o a sus expedientes académicos en soporte papel para el ejercicio de su actividad profesional). En este sentido, no es necesario que exista una dependencia laboral, funcionarial o administrativa indefinida para que la persona con acceso al fichero esté sometida al deber de secreto, el desempeño de cualquier prestación o trabajo que permita el acceso a datos de carácter personal (por ejemplo, datos del alumnado del centro) genera automáticamente la obligación de cumplir con este principio.

De igual manera, no debe confundirse este deber de secreto con el secreto profesional al que están sometidas determinadas personas en función de la profesión que ejercen. Este deber de secreto es un deber genérico que alcanza a cualquier persona que intervenga en el tratamiento de los datos, ya sea personal docente, psicólogos/as, pedagogos/as, logopedas y orientadores/as escolares, personal administrativo, conserjes, personal de limpieza o cualquier otro.

La AEPD, en su Resolución E/01127/2005, de 7 de septiembre de 2006, Fundamento de Derecho IV, ha abundado en el contenido del deber de

secreto establecido en el art. 10 LOPD, señalando lo siguiente:

"Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que, por parte de quienes están en contacto con los datos personales almacenados en ficheros, se realicen filtraciones de los datos no consentidas por los titulares de los mismos".

En este sentido, la Sentencia de la Audiencia Nacional, de fecha 18/01/2002, recoge en su Fundamento de Derecho Segundo, segundo y tercer párrafo: *"El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo"* (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un *"instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos".* Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida.

7. Principio de Seguridad

La Ley Orgánica 2/2006, de 3 de mayo, de Educación, establece expresamente que *"en el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad"*. En este sentido, el art. 9 LOPD, bajo la rúbrica de *"Seguridad de los datos"*, establece que *"el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural"*. Asimismo, el citado artículo señala que *"no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas"*.

De tal manera, conforme a lo establecido en la Ley Orgánica 15/1999, tendrá la consideración de infracción grave, *"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen"* (art. 44.3.h). En este sentido, tal y como se señala en la Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección Primera, núm. Recurso: 1182/2001, de fecha 7 de febrero de 2003, Fundamento de Derecho Tercero, *"No basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva"*.

Con respecto al desarrollo reglamentario de las condiciones o medidas de seguridad a que hacen referencia los artículos 9 y 44.3.h) de la Ley Orgánica 15/1999, señalar que la normativa española sobre Protección de Datos de Carácter Personal se ha caracterizado durante un gran número de años por un cierto desfase en este sentido. De tal manera, la normativa de desarrollo de la antigua Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal (LORTAD) fue

aprobada en 1999 (siete años después de la publicación de la misma), que precisamente fue el mismo año en que apareció la Ley Orgánica 15/1999, que derogaba a la anterior. Debido a ello, se optó por mantener vigente la normativa de desarrollo de la derogada LORTAD, el Real Decreto 994/1999, de 11 de junio, por el que se aprobó el Reglamento de medidas de seguridad de los ficheros automatizados que contuviesen datos de carácter personal, dándose la extraña circunstancia de que mientras la Ley Orgánica 15/1999 tenía por objeto regular tanto los tratamientos automatizados como no automatizados de datos de carácter personal, tan sólo existía desarrollo reglamentario de medidas de seguridad para los ficheros automatizados de datos, quedando un vacío legal para la protección de los ficheros manuales o no automatizados en soporte papel que contuviesen datos de carácter personal.

Tras más de ocho años en la situación descrita, finalmente se ha aprobado el 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, con entrada en vigor el 19 de abril de 2008, y que contempla un catálogo definitivo de medidas de seguridad aplicables tanto a los ficheros y tratamientos automatizados como no automatizados de datos de carácter personal.

De tal manera, el Real Decreto 1720/2007 recoge en su Título VIII toda una serie de medidas de seguridad técnicas y organizativas que los centros de enseñanza deberán adoptar en orden a proteger los datos de carácter personal gestionados en los mismos. A este respecto, el citado Real Decreto establece tres niveles de seguridad (básico, medio y alto), atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

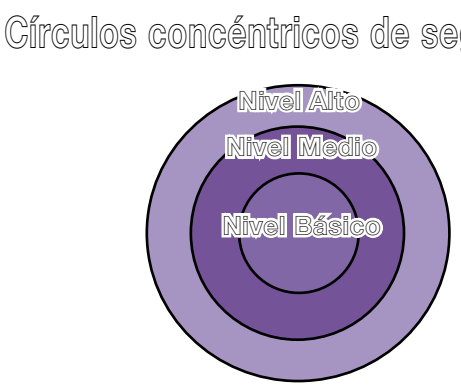
A continuación, procedemos a presentar un esquema comparativo de los niveles de seguridad contemplados en el antiguo Real Decreto 994/1999 y en el nuevo Real Decreto 1720/2007, que deroga al anterior:

REAL DECRETO 994/1999, DE 11 DE JUNIO	
NIVEL BÁSICO	*"Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico"* (art.4.1).
NIVEL BÁSICO CUALIFICADO O NIVEL MEDIO ATENUADO	Se trata de una categoría intermedia, a caballo entre el nivel básico y el nivel medio. El Real Decreto 994/1999 no se refiere expresamente a él como tal, es un nivel puesto de relieve por la doctrina que no está oficialmente reconocido por la Agencia Española de Protección de Datos: *"Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20"* (art. 4.4).
NIVEL MEDIO	*"Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el articulo 28 de la Ley Orgánica 5/1992* (actual artículo 29 de la Ley Orgánica 15/1999, relativo a la Prestación de servicios de información sobre solvencia patrimonial y crédito)*, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio"* (art. 4.2).
NIVEL ALTO	*"Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto"* (art. 4.3).

REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE	
NIVEL BÁSICO	*"Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico"* (art. 81.1). *"En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:* *a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.* *b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad"* (art. 81.5). *"También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes 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"* (art. 81.6).
NIVEL MEDIO	*"Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:* *a) Los relativos a la comisión de infracciones administrativas o penales.* *b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.* *c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.* *d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.* *e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.* *f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos"* (art. 81.2).

NIVEL MEDIO + REGISTRO DE ACCESOS (ART. 103)	*"A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento"* (art. 81.4).
NIVEL ALTO	*"Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:* *a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.* *b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.* *c) Aquéllos que contengan datos derivados de actos de violencia de género"* (art. 81.3).

Una vez encajados en unos u otros niveles cada uno de los ficheros de datos manejados en el centro de enseñanza, se debe proceder a implementar las medidas de seguridad correspondientes en función del nivel asignado. Sobre la adopción de las medidas de índole técnica, organizativa y de gestión encaminadas a garantizar la seguridad de los datos de carácter personal objeto de tratamiento, el Título VIII del Real Decreto 1720/2007 se basa en un esquema de círculos concéntricos. De tal manera, las medidas de seguridad contempladas en el Real Decreto 1720/2007 tienen carácter acumulativo, debiendo adoptarse las medidas correspondientes al nivel aplicable, así como todas aquéllas recogidas en los niveles inferiores:



En el núcleo de este esquema se encontrarían las medidas de seguridad de nivel básico, aplicables a todos los ficheros o tratamientos de datos de carácter personal con carácter general.

Asimismo, en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. Así por ejemplo, bastaría aplicar las medidas de seguridad de nivel básico sobre aquellos ficheros de personal que contuviesen el dato de afiliación a un sindicato (dato especialmente protegido), necesario para el pago de la cuota sindical a través de la nómina salarial (por ejemplo, de un docente afiliado a un sindicato).

- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes 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. Así por ejemplo, sobre un fichero de personal que contenga el dato del grado de minusvalía (dato especialmente protegido de salud) de un docente con una discapacidad auditiva, dato cuya declaración es necesaria para el cálculo de las retenciones prevista en

la legislación del IRPF, bastaría la aplicación de las medidas de seguridad de nivel básico.

Siguiendo con el esquema de círculos concéntricos de seguridad, en la capa intermedia encontraríamos las medidas de seguridad de nivel medio, aplicables a los siguientes ficheros o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.

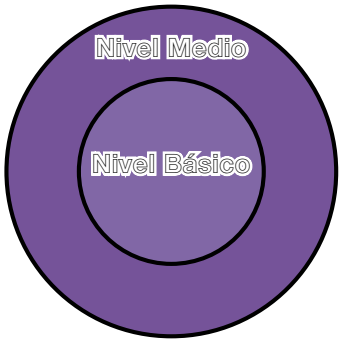
- Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre (Prestación de servicios de información sobre solvencia patrimonial y crédito).

- Aquéllos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

- Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

- Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

- Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.



De tal manera, a los ficheros y tratamientos de datos de carácter personal que tengan encaje en el nivel medio recogido en el Real Decreto 1720/2007, le serían de aplicación las medidas de seguridad tanto de nivel básico como de nivel medio.

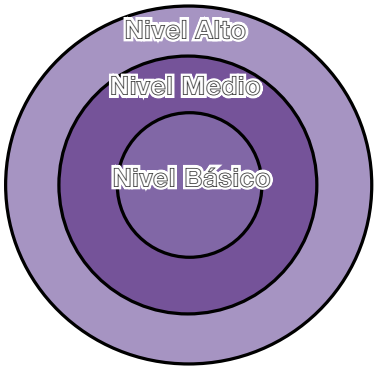
En lo que respecta a los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 del Real Decreto 1720/2007, relativa al *"Registro de accesos"*.

Finalmente, en la capa externa del esquema de círculos concéntricos en que se basa el Título VIII del Real Decreto 1720/2007, se encontrarían las medidas de seguridad de nivel alto, aplicables a los siguientes ficheros o tratamientos de datos de carácter personal:

- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, con las excepciones anteriormente señaladas.

- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

- Aquéllos que contengan datos derivados de actos de violencia de género.



Volvemos a recordar que las medidas de seguridad contempladas en el Título VIII del Real Decreto 1720/2007 tienen carácter acumulativo, de manera que a los datos de carácter personal de nivel alto le son de aplicación las medidas de seguridad de nivel básico, medio y alto.

Recordar, asimismo, que las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

Asimismo, el Real decreto 1720/2007 contempla la posibilidad de que, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de

seguridad diferente al del sistema principal, puedan segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Las medidas de seguridad contempladas en el 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, se dividen en medidas de carácter general aplicables a todos los ficheros y tratamientos de carácter personal (automatizados y no automatizados), medidas aplicables a ficheros y tratamientos automatizados y medidas aplicables a ficheros y tratamientos no automatizados. A su vez, dichas medidas se encajan en cada uno de los diferentes niveles anteriormente comentados (básico, medio o alto).

Al igual que en el anterior Real Decreto 994/1999, existe la obligación por parte del responsable del fichero o tratamiento de elaborar e implantar un documento, de obligado cumplimiento para el personal con acceso a los sistemas de información, que recoja las medidas de índole técnica y organizativa encaminadas a garantizar la seguridad de los datos de carácter personal objeto de tratamiento, el llamado "Documento de Seguridad". Sobre el contenido mínimo del citado documento, su actualización, adecuación a las disposiciones vigentes en materia de seguridad de los datos de carácter personal y otros aspectos formales del mismo, el artículo 88 del Real Decreto 1720/2007 desgrana en profundidad éstas y otras cuestiones de interés acerca del mismo:

"Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad

agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

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 este reglamento.

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) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del

encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal."

Una novedad importante con respecto al anterior Real Decreto 994/1999, es la posibilidad que ofrece el Real Decreto 1720/2007 de delegar, en aquellos casos en que la totalidad de los ficheros o tratamientos del responsable se incorporen y traten de modo exclusivo en los sistemas del encargado, la llevanza del documento de seguridad en el encargado del tratamiento, salvo en lo relativo a aquellos datos de carácter personal contenidos en recursos propios del responsable.

Con respecto a las medidas de seguridad aplicables a los ficheros automatizados de datos de carácter personal, éstas son semejantes a las contempladas en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, clasificándose, asimismo, en medidas de seguridad de nivel básico, medio y alto. De manera sintética, podemos resumir dichas medidas de seguridad en las siguientes:

7. 1. Ficheros automatizados.

7. 1. 1. Medidas de seguridad de Nivel Básico:

- Definición y documentación de las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información.

- Adopción de las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- Generación de un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecimiento de un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

- Establecimiento de mecanismos de control de acceso a los datos y recursos por parte de los usuarios.

- Cumplimiento de medidas relativas a la gestión de soportes que contengan datos de carácter personal (inventariado e identificación, salidas, traslado, destrucción, etc.), entendiendo por soporte cualquier objeto físico que almacene o contenga datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos. Dichas medidas son igualmente aplicables a los soportes o documentos comprendidos y/o anejos a un correo electrónico.

- Implantación de un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado (por ejemplo, usuario y contraseña).

- Realización de copias de respaldo y recuperación de los datos con una periodicidad mínima semanal, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos. Verificación cada seis meses de la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

- Prohibición de realizar con datos reales pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado, se anote su realización en el documento de seguridad y se haya realizado previamente una copia de seguridad.

7. 1. 2. Medidas de Seguridad de Nivel Medio:

- Cumplimiento de las medidas de seguridad de nivel básico. Recordamos, en este sentido, que las medidas de seguridad contempladas en el Título VIII del Real Decreto 1720/2007 tienen carácter acumulativo, debiendo adoptarse las medidas correspondientes al nivel aplicable, así como todas aquéllas recogidas en los niveles inferiores.

- Designación de uno, una o varios, varias responsables de seguridad, encargados de coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

- Sometimiento de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos a una auditoria interna o externa que verifique el cumplimiento del Título VIII del Real Decreto 1720/2007, al menos, cada dos años. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen

modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.

- Establecimiento de un sistema de registro de entrada y salida de soportes, entendiendo por soporte cualquier objeto físico que almacene o contenga datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

- Establecimiento de un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
- Establecimiento de mecanismos de control de acceso físico a los lugares donde se hallen instalados los equipos que den soporte a los sistemas de información. Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los mismos.

- Cumplimiento de medidas adicionales con respecto al registro de incidencias, debiendo consignarse los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

7. 1. 3. Medidas de Seguridad de Nivel Alto:

- Cumplimiento de las medidas de seguridad de nivel básico y de nivel medio. Recordamos, en este sentido, que las medidas de seguridad contempladas en el Título VIII del Real Decreto 1720/2007 tienen carácter acumulativo, debiendo adoptarse las medidas correspondientes al nivel aplicable, así como todas aquéllas recogidas en los niveles inferiores.
- Identificación de los soportes que contengan datos de carácter personal utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que

dificulten la identificación para el resto de personas. Distribución de los mismos cifrando los datos que contengan o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

- Cifrado de los datos de carácter personal que contengan los dispositivos portátiles (ordenadores portátiles, PDAs, etc.), cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

- Conservación de una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en el Título VIII del Real Decreto 1720/2007, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

- Implementación de un registro de accesos que deberá guardar, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Revisión, al menos una vez al mes, de la información de control registrada y elaboración de un informe de las revisiones realizadas y los problemas detectados.

- Cifrado de los datos de carácter personal, o utilización de cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros, cuando se transmitan a través de redes públicas o redes inalámbricas de comunicaciones electrónicas (por ejemplo, Internet).

Asimismo, el Título VIII del Real Decreto 1720/2007 contempla, con carácter adicional, otra serie de medidas de seguridad aplicables a cualquier fichero o tratamiento automatizado de datos de carácter personal, con independencia del nivel en el cual tengan encaje los mismos:

- Garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local cuando el acceso a los datos de carácter personal se realice a través de redes de comunicaciones, sean o no públicas.

- Cuando los datos de carácter personal se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento o del encargado del tratamiento, será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

- Aquellos ficheros temporales que se creen exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir con las medidas de seguridad correspondientes, de conformidad con el nivel aplicable en base a lo establecido en el Real Decreto 1720/2007. Asimismo, deberán ser borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

En lo que respecta a las medidas de seguridad aplicables a los ficheros no automatizados que contengan datos de carácter personal, éstas se clasifican, de manera semejante a las contempladas para los ficheros automatizados, en medidas de seguridad de nivel básico, medio y alto:

7. 2. Ficheros no automatizados.

7. 2. 1. Medidas de seguridad de Nivel Básico:

- Definición y documentación de las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información.

- Adopción de las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que

pudiera incurrir en caso de incumplimiento.

- Generación de un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecimiento de un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

- Establecimiento de mecanismos de control de acceso a los datos y recursos por parte de los usuarios.

- Cumplimiento de medidas relativas a la gestión de documentos que contengan datos de carácter personal (inventariado e identificación, salidas, traslado, destrucción, etc.), entendiendo por documento todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

- El archivo de los documentos deberá realizarse de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

- Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura (por ejemplo, sistema de apertura mediante llave u otro dispositivo equivalente). Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

- Mientras la documentación con datos de carácter personal no se encuentre archivada en dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

7. 2. 2. Medidas de Seguridad de Nivel Medio:

- Cumplimiento de las medidas de seguridad de nivel básico. Recordamos, en este sentido, que las medidas de seguridad contempladas en el Título VIII del Real Decreto 1720/2007 tienen carácter acumulativo, debiendo adoptarse las medidas correspondientes al nivel aplicable, así como todas aquéllas recogidas en los niveles inferiores.

- Designación de uno, una o varios, varias responsables de seguridad, encargados de coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

- Sometimiento de los ficheros de datos de carácter personal a una auditoria interna o externa que verifique el cumplimiento del Título VIII del Real Decreto 1720/2007, al menos, cada dos años.

7. 2. 3. Medidas de Seguridad de Nivel Alto:

- Cumplimiento de las medidas de seguridad de nivel básico y de nivel medio. Recordamos, en este sentido, que las medidas de seguridad contempladas en el Título VIII del Real Decreto 1720/2007 tienen carácter acumulativo, debiendo adoptarse las medidas correspondientes al nivel aplicable, así como todas aquéllas recogidas en los niveles inferiores.

- Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

- La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad. Asimismo, deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

- El acceso a la documentación se limitará exclusivamente al personal autorizado. Se deberán establecer mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

- Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Finalmente, el Título VIII del Real Decreto 1720/2007 contempla, con carácter adicional, otra serie de medidas de seguridad aplicables a cualquier fichero o tratamiento no automatizado de datos de carácter personal, con independencia del nivel en el cual tengan encaje los mismos:

- Cuando los datos de carácter personal se traten fuera de los locales del responsable de fichero o tratamiento o del encargado del tratamiento, será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

- Aquellas copias de documentos que se creen exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir con las medidas de seguridad correspondientes, de conformidad con el nivel aplicable en base a lo establecido en el Real Decreto 1720/2007. Asimismo, deberán ser destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD			
NIVEL	**MEDIDA DE SEGURIDAD**	**AUTOM.**	**NO AUTOM.**
COMÚN	Encargado del tratamiento	✓	✓
COMÚN	Prestaciones de servicios sin acceso a datos personales	✓	✓
COMÚN	Delegación de autorizaciones	✓	✓
COMÚN	Acceso a datos a través de redes de comunicaciones	✓	
COMÚN	Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento	✓	✓
COMÚN	Ficheros temporales o copias de trabajo de documentos	✓	✓
BÁSICO	Documento de seguridad	✓	✓
BÁSICO	Funciones y obligaciones del personal	✓	✓
BÁSICO	Registro de incidencias	✓	✓
BÁSICO	Control de acceso	✓	✓
BÁSICO	Gestión de soportes y documentos	✓	✓
BÁSICO	Identificación y autenticación	✓	
BÁSICO	Copias de respaldo y recuperación	✓	
BÁSICO	Criterios de archivo		✓
BÁSICO	Dispositivos de almacenamiento		✓
BÁSICO	Custodia de los soportes		✓
MEDIO	Responsable de seguridad	✓	✓
MEDIO	Auditoría	✓	✓
MEDIO	Gestión de soportes y documentos	✓	
MEDIO	Identificación y autenticación	✓	
MEDIO	Control de acceso físico	✓	
MEDIO	Registro de incidencias	✓	
ALTO	Gestión y distribución de soportes	✓	
ALTO	Copias de respaldo y recuperación	✓	
ALTO	Registro de accesos	✓	
ALTO	Telecomunicaciones	✓	
ALTO	Almacenamiento de la información		✓
ALTO	Copia o reproducción		✓
ALTO	Acceso a la documentación		✓
ALTO	Traslado de documentación		✓

CAPÍTULO IV

RECOMENDACIONES PARA EL CORRECTO TRATAMIENTO DE FICHEROS NO AUTOMATIZADOS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

1. Introducción

Si bien es cierto que los centros de enseñanza de la Junta de Andalucía están siendo objeto de un irreversible proceso de informatización que les permite beneficiarse de las ventajas que ofrecen las nuevas Tecnologías de la Información y las Comunicaciones (TICs), no podemos obviar que en los mismos todavía se maneja una gran cantidad de documentación en formato papel: los formularios de solicitud de plaza y matriculación, expedientes académicos, informes psicopedagógicos y test de inteligencia y conducta elaborados por los orientadores y orientadoras, fichas manejadas por el profesorado, listados de diversa naturaleza, etc. Esta circunstancia debe hacernos reflexionar acerca de la necesidad de proteger, al igual que los datos de carácter personal automatizados, la documentación en papel que contenga información concerniente a personas físicas identificadas o identificables (por ejemplo, alumnado del centro).

En este sentido, debemos señalar que la normativa española sobre Protección de Datos de Carácter Personal se ha caracterizado durante un gran número de años por un cierto desfase en este sentido. De tal manera, la normativa de desarrollo de la antigua Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal (LORTAD) fue aprobada en 1999 (siete años después de la publicación de la misma), que precisamente fue el mismo año en que apareció la Ley Orgánica 15/1999, que derogaba a la anterior. Debido a ello, se optó por mantener vigente la normativa de desarrollo de la derogada LORTAD, el Real Decreto 994/1999, de 11 de junio, por el que se aprobó el Reglamento de medidas de seguridad de los ficheros automatizados que contuviesen datos de carácter personal, dándose la extraña circunstancia de que mientras la Ley Orgánica 15/1999 tenía por objeto regular tanto los tratamientos automatizados como no automatizados de datos de carácter personal, tan sólo existía desarrollo reglamentario de medidas de seguridad para los ficheros automatizados de datos, quedando un vacío legal para la protección de los ficheros manuales o no automatizados en formato papel que contuviesen datos de carácter personal.

A la espera de la aprobación del desarrollo reglamentario de la Ley Orgánica 15/1999, que contemplase un catálogo de medidas de seguridad aplicables a los ficheros no automatizados que contuviesen datos de carácter personal, la Agencia Española de Protección de Datos entendió que debían trasladarse las medidas contempladas para los ficheros automatizados de datos también a los no automatizados, en la medida que fuera posible:

"En lo que se refiere a la aplicación de las medidas de seguridad exigidas por el Reglamento debe formularse una aclaración respecto a su aplicación en los ficheros no automatizados.

El artículo 1 del Reglamento delimita su ámbito de aplicación estableciendo que será aplicable únicamente a los ficheros automatizados. Esta delimitación resultaba congruente con el sistema de garantías contemplado en la Ley Orgánica 5/1992, de 29 de octubre (LORTAD), en cuyo desarrollo fue aprobado, y que sólo era de aplicación a ficheros automatizados.

La vigente LOPD presenta como una de sus principales novedades la ampliación de su ámbito de aplicación que ahora alcanza "los datos de carácter personal registrados en soporte físico que los hace susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos..." (art. 2). Incluye, por tanto, los datos en soporte papel siempre que estén estructurados como ficheros.

La Disposición Transitoria Tercera de la LOPD mantiene la vigencia de las normas reglamentarias preexistentes, entre las que se cita el Reglamento de Medidas de Seguridad, en cuanto no se oponga a la nueva Ley.

La previsión del Reglamento de aplicarse sólo a los ficheros automatizados se opone a la vigente LOPD, al haberse ampliado su ámbito de aplicación, como se ha expuesto, por lo que debe considerarse derogada.

En consecuencia, desde la entrada en vigor de la LOPD, resulta aplicable dicho Reglamento a los ficheros en soporte no automatizado que se hubieran creado con posterioridad a la entrada en vigor de la Ley Orgánica, el 14 de enero

de 2000. Los ficheros en soportes no automatizados que existieran antes de dicha fecha dispondrán, a estos efectos, del período de adaptación establecido en la Disposición Adicional Primera (que finaliza en octubre de 2007).

No obstante, cuando resulte de aplicación el Reglamento de Medidas de Seguridad, conforme a los criterios expuestos, sólo deberán implantarse las medidas de seguridad que, pese a estar previstas para tratamientos automatizados, por su naturaleza sean también aplicables a ficheros no automatizados como, por ejemplo, la elaboración e implantación del Documento de Seguridad".

Ahora bien, la aplicación analógica de las medidas de seguridad previstas para los ficheros automatizados de datos a los ficheros no automatizados que contuviesen datos de carácter personal no era algo sencillo, ya que se trataba de medidas especialmente concebidas para un entorno basado en la tecnología digital.

Tras más de ocho años en la situación descrita, finalmente se ha aprobado el 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, con entrada en vigor el 19 de abril de 2008, y que contempla un catálogo definitivo de medidas de seguridad aplicables tanto a los ficheros y tratamientos automatizados como no automatizados de datos de carácter personal.

De tal manera, el Real Decreto 1720/2007 recoge en el Capítulo IV de su Título VIII toda una serie de medidas de seguridad que los centros de enseñanza deberán adoptar en orden a proteger los datos de carácter personal gestionados en sus ficheros manuales o no automatizados en formato papel. En este sentido, el citado Real Decreto entiende por fichero no automatizado *"todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica"* (art. 5.1.n).

A este respecto, el Capítulo IV del Título VIII del Real Decreto 1720/2007 establece tres niveles de seguridad distintos (básico, medio y alto), atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de los datos de carácter personal contenidos en los ficheros no automatizados.

Recordar asimismo que, conforme a lo establecido en la Ley Orgánica 15/1999, tendrá la consideración de infracción grave, *"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen"* (art. 44.3.h)). En este sentido, tal y como se señala en la Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección Primera, núm. Recurso: 1182/2001, de fecha 7 de febrero de 2003, Fundamento de Derecho Tercero, *"No basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva"*.

2. Recomendaciones sobre protección de la documentación en formato papel

2.1. Indicaciones Generales

Por encima de cualquier otra consideración, los centros de enseñanza deben ser conscientes de la importancia de preservar la integridad y confidencialidad de los documentos en formato papel que contengan datos de carácter personal y evitar su pérdida, destrucción o accesos no autorizados a los mismos, frente a los riesgos de una pérdida de información definitiva –volver a generar un documento idéntico o recuperar la información en él contenida es una tarea infinitamente más compleja que en el mundo digital, ya que aquí no existe la posibilidad de realizar copias de seguridad– o accesos indebidos de terceros a la información que puedan contener los documentos.

Por lo tanto, es un factor importante para cualquier centro educativo tener bien documentado el procedimiento de generación, uso y destrucción de los documentos en formato papel que contengan información concerniente a personas físicas identificadas o identificables, así como el conjunto de medidas adoptadas para garantizar la integridad, confidencialidad y disponibilidad de los mismos, su archivo y gestión y las condiciones de acceso a la información que contengan.

En este sentido, el art. 106 del Real Decreto 1720/2007, relativo a los *"Criterios de archivo"*, establece que *"El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación"*. En aquellos casos en los que no exista norma aplicable, *"el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo"*.

A este respecto, el Real Decreto 1720/2007 entiende por documento *"todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada"* (por ejemplo, un informe psicopedagógico o un formulario de solicitud de plaza) y por soporte el *"objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos"* (art. 5.2 letras f) y ñ) respectivamente).

2.2. Niveles de Seguridad establecidos en el REAL DECRETO 1720/2007

Con respecto a las medidas de seguridad que se vayan a adoptar para proteger los ficheros no automatizados que contengan datos de carácter personal, es muy importante tener en cuenta que no todos los documentos contienen el mismo tipo de información. En este sentido, el 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, establece diferentes niveles de seguridad en función del tipo de datos de que estemos hablando:

Nivel Básico

Aplicable a cualquier fichero que contenga datos de carácter personal, esto es, cualquier información concerniente a personas físicas identificadas o identificables. Así por ejemplo, tendrían cabida dentro de esta categoría el

nombre y apellidos de los alumnos y alumnas, el número de su Documento Nacional de Identidad, dirección, teléfono, fecha y lugar de nacimiento, sexo, datos de familia, historial de estudiante, calificaciones, etc. El dato acerca de si un alumno o alumna del centro de enseñanza es adoptado o adoptada también tendría encaje en el nivel básico de medidas de seguridad, lo cual no es obstáculo para que dicha información sea tratada con una especial sensibilidad, por las posibles consecuencias que podría tener para el menor su revelación a terceros malintencionados.

Asimismo, en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. Así por ejemplo, bastaría aplicar las medidas de seguridad de nivel básico sobre aquellos ficheros de personal que contuviesen el dato de afiliación a un sindicato (dato especialmente protegido), necesario para el pago de la cuota sindical a través de la nómina salarial (por ejemplo, de un docente afiliado a un sindicato).

- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes 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. Así por ejemplo, sobre un fichero de personal que contenga el dato del grado de minusvalía (dato especialmente protegido de salud) de un docente con una discapacidad auditiva, dato cuya declaración es necesaria para el cálculo de las retenciones prevista en la legislación del IRPF, bastaría la aplicación de las medidas de seguridad de nivel básico.

Nivel Medio

Aplicable a los siguientes ficheros o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.

- Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre (Prestación de servicios de información sobre solvencia patrimonial y crédito).

- Aquéllos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

- Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

- Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

- Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

Como puede deducirse, en el caso de un centro de enseñanza, la adopción de las medidas de seguridad de nivel medio sólo será necesaria en aquellos supuestos en que el fichero en cuestión contenga un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los alumnos y alumnas del centro (o, en su caso, de otro tipo de personas físicas, por ejemplo, de los docentes, si bien éste es un supuesto mucho más improbable) y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. En este

sentido, la Real Academia Española de la Lengua define la *"personalidad"*, entre otras acepciones, como el *"conjunto de cualidades que constituyen a la persona o sujeto inteligente"*.

De tal manera, los informes psicopedagógicos elaborados por los orientadores y orientadoras podrían encajar dentro del nivel medio definido en el Real Decreto 1720/2007, ya que contienen un conjunto de datos de carácter personal que ofrecen una definición de las características o de la personalidad de los alumnos y alumnas del centro y que permiten evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. Ahora bien, los datos psicológicos tienen, como veremos, la consideración de datos de salud, debiendo adoptarse, en su consecuencia, las medidas de seguridad de nivel alto definidas en el Real Decreto 1720/2007 (el nivel alto prevalece sobre los restantes).

Que las medidas de seguridad a adoptar sean las de nivel medio, se desprende del reciente Informe del Gabinete Jurídico de la Agencia Española de Protección de Datos (Informe 0572/2009) que establece: *"Esta Agencia ha venido señalando respecto a la interpretación que debe darse al artículo 81.2.f) que de dicho precepto se desprende que su finalidad es someter a criterios de seguridad más rigurosos aquellos ficheros que permitan obtener una información adicional sobre el afectado, obteniendo así un perfil de situación económica o familiar o de sus aficiones, preferencias, etc. Así, se encontrarán comprendidos en dicho artículo todos los ficheros que contengan datos a partir de los cuales puedan deducirse cualquiera de las facetas antes mencionadas o, como sucede en el presente caso, se incluyan datos relativos al rendimiento académico que permitan deducir un perfil de estudios."*

Nivel Alto

Aplicable a los siguientes ficheros o tratamientos de datos de carácter personal:

- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, con las excepciones anteriormente señaladas.

- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

- Aquéllos que contengan datos derivados de actos de violencia de género.

En principio, podemos pensar que estas categorías de datos están exclusivamente reservadas para centros sanitarios y hospitalarios, sindicatos, partidos políticos, confesiones religiosas, fuerzas y cuerpos de seguridad, centros de atención a la mujer maltratada, etc.: nada más lejos de la realidad.

Como ya hemos indicado, los orientadores y orientadoras suelen confeccionar informes psicopedagógicos, test de inteligencia y conducta, etc. Para su elaboración, es necesario recabar una serie de información concerniente a cada uno de los alumnos y alumnas del centro, incluyendo datos psicológicos.

Con respecto a la naturaleza de los datos psicológicos, la cuestión radica en delimitar si procede su inclusión dentro del concepto de datos referentes a la salud de las personas. Si bien la Ley Orgánica se refiere expresamente a los datos de salud, considerándolos expresamente protegidos y limitando la posibilidad de su recopilación y cesión, no establece un concepto concreto de este tipo de datos. En este sentido, la Agencia Española de Protección de Datos ha entendido que los datos psicológicos deben ser considerados, a los efectos de la aplicación de la LOPD, como datos relativos a la salud de las personas, habida cuenta que, o bien conciernen directamente a la salud mental del individuo o bien se encuentran estrechamente relacionados con la salud.

En consecuencia, la AEPD entiende que los datos de carácter psicológico han de ser considerados datos especialmente protegidos referentes a la salud de las personas, regulados en el artículo 7.3 LOPD.

De hecho, el Informe 0572/2009, del Gabinete Jurídico de la Agencia Española de Protección de Datos, referente a las medidas de seguridad

aplicables a los ficheros con datos académicos, dice textualmente: *"No obstante, debe indicarse que si el fichero contuviera datos referentes al perfil psicológico de los afectados y que hicieran referencia a la existencia de anomalías o especialidades de la personalidad del sujeto, habrá de considerarse que el fichero contiene datos relacionados con la salud de las personas, siendo entonces de aplicación lo dispuesto en el artículo 81.3.a) del Reglamento 1720/2007, que exige la adopción sobre estos ficheros de las medidas de seguridad de nivel alto, además de las medidas de nivel básico y medio".*

Por tanto, de acuerdo a la interpretación de la AEPD, el nivel de protección que correspondería a los datos contenidos en los informes psicopedagógicos en formato papel sería nivel alto.

El reciente Real Decreto 1720/2007 sí recoge, a diferencia de la Ley Orgánica 15/1999, una definición de *"Datos de carácter personal relacionados con la salud"*, entendiendo por tales *"las 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"* (art. 5.1.g)).

A este respecto, cabe citar las siguientes normas autonómicas:

- El Decreto 213/1995, de 12 de septiembre, por el que se regulan los Equipos de Orientación Educativa.

- La Orden de 23 de julio de 2003, por la que se regulan determinados aspectos sobre la organización y el funcionamiento de los Equipos de Orientación Educativa.

- El Reglamento Orgánico de los Institutos de Educación Secundaria, aprobado por Decreto 200/1997, de 3 de septiembre, que establece la composición y funciones de los Departamentos de Orientación, así como las funciones de los orientadores u orientadoras.

- La Orden de 27 de julio de 2006, por la que se regulan determinados aspectos referidos a la organización y funcionamiento del departamento de orientación en los Institutos de Educación Secundaria.

Sobre los Equipos de Orientación Educativa, el Decreto 213/1995 los define como *"unidades básicas de orientación psicopedagógica que, mediante el desempeño de funciones especializadas en las áreas de orientación educativa, atención a los alumnos y alumnas con necesidades educativas especiales, compensación educativa y apoyo a la función tutorial del profesorado, actúan en el conjunto de los centros de una zona"* (art. 1).

En lo que respecta a los Departamentos de Orientación, el Reglamento Orgánico de los Institutos de Educación Secundaria asigna a los mismos la función de elaborar la propuesta del Plan de Orientación y Acción Tutorial, así como un conjunto de funciones relacionadas con la orientación académica, psicopedagógica y profesional, con la evaluación psicopedagógica de los alumnos y alumnas que la requieran y con el apoyo a la Acción Tutorial, todo ello en el marco de la atención a las diversas aptitudes, intereses y motivación del alumnado.

Por citar un ejemplo, el expediente académico de un alumno o una alumna con necesidades educativas especiales puede contener el certificado del grado de su minusvalía, copia de su historia clínica y el dictamen de escolarización, además de los informes psicopedagógicos elaborados por los orientadores y orientadoras, todos ellos considerados datos especialmente protegidos.

Al margen de los datos psicológicos, en un centro de enseñanza pueden encontrarse toda otra serie de datos relativos a la salud del alumnado en formato papel. Así por ejemplo, si en el comedor escolar disponen de fichas en papel donde figuren alergias a determinados alimentos de algunos alumnos y alumnas estaríamos ante datos de salud catalogados como de nivel alto. En idéntica situación estaríamos si en el centro de enseñanza se dispusiera de información sobre determinados alumnos y alumnas que presenten problemas de salud que les imposibilite el ejercicio físico, por ejemplo.

Igualmente, cabe la posibilidad de que algún centro de enseñanza maneje información sobre el origen racial de algunos alumnos y alumnas. Señalar que, en este caso, también estaríamos ante datos catalogados de nivel alto.

Finalmente, queda la incógnita de si el hecho de cursar la asignatura de religión, o el hecho de no cursarla, suponen la revelación de un dato protegido por el derecho fundamental a la libertad religiosa, consagrado por el artículo 16.1 de la Constitución, es decir, si ese dato revela efectivamente las convicciones religiosas de la persona a la que se refiere y, por tanto, merece la catalogación de dato especialmente protegido. Según la AEPD, el hecho mismo de cursar la asignatura de religión no revela necesariamente que el estudiante profese las creencias a las que tal asignatura se refiere, del mismo modo que el hecho de no cursarla no revela la inexistencia de esas creencias, sino que tal circunstancia puede deberse al estudio de la religión en otros foros distintos del escolar. Es decir, a juicio de la AEPD, lo único que revela el dato de optar por cursar la asignatura de religión sería el interés del alumno o la alumna por conocer los principios, historia y preceptos de la misma, sin que ello implique una efectiva confesionalidad del mismo o la misma, a cuya declaración no podría encontrarse obligado u obligada.

En definitiva, según la AEPD, el dato relacionado con el hecho de que el alumno o la alumna curse la asignatura de religión, no vinculada a la participación del alumno o la alumna en un rito relacionado con una religión determinada (lo que sí implicaría que el individuo profesa dicha creencia religiosa) no puede ser considerado por sí mismo un dato que revele inmediatamente las creencias religiosas del afectado o la afectada, por lo que el dato de opción por la asignatura de Religión no tendría la naturaleza de especialmente protegido.

En su consecuencia, un documento en formato papel que contenga el dato relativo a la opción por la asignatura de religión debe encajarse dentro del nivel básico contemplado en el Real Decreto 1720/2007.

2.3. Medidas de seguridad

Una vez encajados en cada uno de los niveles descritos los distintos ficheros no automatizados de datos de carácter personal objeto de tratamiento en el centro de enseñanza, se debe proceder a la implementación de las medidas de seguridad correspondientes en función del nivel asignado y que se recogen, como ya hemos indicado, en el Capítulo IV del Título VIII del 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. Éstas se clasifican, de manera semejante a las contempladas para los ficheros automatizados, en medidas de seguridad de nivel básico, medio y alto. Asimismo, tienen carácter acumulativo, debiendo adoptarse las medidas correspondientes al nivel aplicable, así como todas aquéllas recogidas en los niveles inferiores.

Una primera medida inexcusable y común a todos los niveles citados sería la de documentar detalladamente el conjunto de medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a la información contenida en los documentos en formato papel. La documentación por escrito de esta serie de medidas daría lugar a la generación de lo que, en términos de la normativa sobre protección de datos de carácter personal, se conoce formalmente como *"Documento de Seguridad"*.

Nivel Básico

Con respecto a las medidas de seguridad tendentes a proteger los documentos que contengan únicamente datos de nivel básico, éstas no deben ser especialmente gravosas, ya que se trata de datos que efectivamente revisten su importancia pero no tienen la trascendencia de otro tipo de datos especialmente protegidos (por ejemplo, datos relativos a la salud del alumnado). Entre dichas medidas, cabe citar, a modo de ejemplo, las siguientes:

- Cada una de las personas que trabajan en el centro de enseñanza deben tener perfectamente delimitadas sus funciones y obligaciones, de tal manera que sólo tengan acceso a aquellos documentos

imprescindibles para el ejercicio de su actividad concreta, ya sea personal docente, de administración, servicios o cualquier otro. En este mismo sentido, en el documento de seguridad debe constar una relación detallada de todo el personal con posibilidad de acceso.

- Asimismo, se deberán adoptar las medidas necesarias para que las personas que trabajan en el centro de enseñanza conozcan de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- Generar un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal contenidos en ficheros no automatizados (por ejemplo, la pérdida de una de las llaves de apertura del lugar donde se almacenen los documentos) y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

- Establecer un mecanismo que permita controlar las salidas y traslado de cualquier clase de documento que contenga datos de carácter personal, con la finalidad de que no se produzca ninguna salida de datos del centro sin la autorización previa de la Dirección del mismo.

- Los dispositivos donde se almacenen los documentos que contengan los datos de carácter personal (por ejemplo, un armario o archivador donde se guarden las fichas del alumnado) deben disponer de algún mecanismo que obstaculice su apertura (por ejemplo, una cerradura con llave o un candado).

  Como es lógico pensar, únicamente deben disponer de una copia de la citada llave aquellas personas que, en el desarrollo de sus funciones, necesiten tener acceso a la información contenida en los documentos. Por citar un ejemplo, carecería de sentido que una persona encargada

de la limpieza del centro dispusiera de una copia de la misma.

- Mientras la documentación con datos de carácter personal no se encuentre archivada en dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura (por ejemplo, el expediente académico de un alumno que está siendo objeto de revisión), la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Nivel Medio

En lo referente a las medidas de seguridad que han de implantarse en el nivel medio recogido en el Real Decreto 1720/2007, señalar que, en principio, deben adoptarse todas las contempladas para el nivel básico, añadiendo, además, las que a continuación se relacionan:

- Designación de uno, una o varios, varias Responsables de Seguridad que se encargue de coordinar y controlar las medidas de seguridad encaminadas a proteger la documentación en formato papel que contenga datos de carácter personal. La persona más idónea para asumir esta función coordinadora es, sin lugar a dudas, alguien que tenga un conocimiento profundo del funcionamiento interno del centro en su conjunto.
- Someterse a auditorías, al menos bienales, de verificación de cumplimiento de la normativa sobre protección de datos de carácter personal. Dichas auditorías pueden ser realizadas por personal externo o bien por personal del propio centro con conocimientos sólidos sobre la normativa.

Nivel Alto

En tercer lugar, con respecto a los documentos en formato papel que contengan datos especialmente protegidos, quedando enmarcados por tanto dentro del nivel alto establecido en el Real Decreto 1720/2007, deberán adoptarse las siguientes medidas de seguridad, con carácter adicional a las anteriormente señaladas para los niveles básico y medio:

- Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero. Asimismo, las llaves de acceso a dichas áreas únicamente deben estar en poder de aquellas personas que, en el desarrollo de sus funciones, necesiten tener acceso a la información contenida en los documentos.

- La generación de copias o la reproducción de los documentos (por ejemplo, el informe psicopedagógico de un alumno o alumna del centro) únicamente podrá ser realizada bajo el control del personal del centro de enseñanza expresamente autorizado en el documento de seguridad. Asimismo, deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

- El acceso a la documentación en formato papel se limitará exclusivamente a las personas autorizadas que trabajan en el centro de enseñanza. Se deberán establecer mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

- Siempre que se proceda al traslado físico de documentación en formato papel que contenga datos de carácter personal especialmente protegidos, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Finalmente, el Título VIII del Real Decreto 1720/2007 contempla, con carácter adicional, otra serie de medidas de seguridad aplicables a cualquier fichero o tratamiento no automatizado de datos de carácter personal, con independencia del nivel en el cual tengan encaje los mismos:

- Cuando los datos de carácter personal se traten fuera de los locales del responsable de fichero o tratamiento (por ejemplo, la corrección

de los exámenes que contienen datos del alumnado fuera del centro, en casa del docente), será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

- Aquellas copias de documentos que se creen exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir con las medidas de seguridad correspondientes, de conformidad con el nivel aplicable en base a lo establecido en el Real Decreto 1720/2007. Asimismo, deberán ser destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

Recordar, asimismo, que las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

En este último sentido, proponemos la implantación de medidas de seguridad adicionales tendentes a evitar o disminuir el riesgo de catástrofes como fuego o incendios, inundaciones o cualquier otra contingencia que pueda ocasionar una pérdida definitiva de la información archivada en formato papel, entre las cuales cabe citar las siguientes:

- Instalación de detectores de humo.

- Provisión de extintores de incendios.

- Utilización de armarios o archivadores metálicos, para evitar incendios.

- La sala o dependencia destinada al archivo y gestión de los documentos no debe estar ubicada en un sótano o planta baja, ya que el riesgo de inundación es mayor.

- Procurar unas condiciones de temperatura y humedad adecuadas.

- Buena ventilación, para evitar gases, humo y polvo.

- Fumigación periódica de la sala o dependencia destinada al archivo y gestión de los documentos, para evitar la aparición de insectos bibliófagos.

Finalmente, todo el personal autorizado que tenga acceso a los documentos en formato papel debe firmar un compromiso de confidencialidad con el centro en relación a dicha documentación, en el cual se responsabilice personalmente de cumplir con la normativa sobre protección de datos. Esta recomendación entronca directamente con el deber de secreto que recoge el art. 10 LOPD para todo aquél que tenga acceso a datos de carácter personal en el desempeño de sus funciones.

3. Recomendaciones sobre destrucción de la documentación

El principio de calidad de los datos establecido en la Ley Orgánica 15/1999 impone que los datos de carácter personal deberán ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados y que no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Es decir, en el caso de un documento en formato papel que contenga datos de carácter personal que ya no sean necesarios para la finalidad que motivó su recogida, éste –salvo norma específica en contrario– debe ser destruido. Además, ello debe hacerse de tal manera que sea imposible la identificación de las personas cuyos datos constaran en el mismo.

En este sentido, el artículo 92 del nuevo 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, relativo a la *"Gestión de soportes y documentos"*, establece que *"siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior"*.

Asimismo, el artículo 112 del citado Real Decreto 1720/2007, que lleva por rúbrica *"Copia o reproducción"*, señala que *"la generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad"* y que *"deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior"*.

Ahora bien, surge entonces la pregunta: ¿cuál es el procedimiento correcto para destruir documentos en formato papel que contengan información concerniente a personas físicas identificadas o identificables, de manera que se evite el acceso a la información contenida en los mismos

o su recuperación posterior? En principio, ni la Ley Orgánica 15/1999 ni el Real Decreto 1720/2007 establecen nada al respecto.

Frente a la citada falta de previsión legislativa, podemos tomar como guía el Documento sobre *Recomendaciones para la destrucción física de documentos de archivo en papel de la Administración General del Estado*, aprobado por la Comisión Superior Calificadora de Documentos Administrativos, en sesión de 27 de noviembre de 2003, el cual, si bien no resulta de aplicación directa a los centros de enseñanza de la Junta de Andalucía, puede servir de excelente apoyo para orientar a los mismos a la hora de destruir cualquier tipo de documentación en formato papel que contenga información concerniente a personas físicas identificadas o identificables con las garantías de confidencialidad debidas.

En concreto, el Documento a que hacemos referencia contiene una serie de previsiones referentes al almacenamiento, transporte y destrucción de la documentación que se vaya a eliminar, así como respecto al tema de las garantías en caso de que se contrate una empresa especializada en servicios de destrucción de documentos.

En primer lugar, se hace referencia a la cuestión del correcto almacenamiento de la documentación que va a ser destruida. En este sentido, se realizan las siguientes recomendaciones:

- Los documentos que vayan a ser eliminados deben estar protegidos hasta el momento de su destrucción física.

- El lugar o los contenedores donde se almacenen los documentos que se vayan a eliminar requerirán medidas de seguridad eficaces frente a posibles intromisiones exteriores. No deben permanecer al descubierto en el exterior de los edificios. Tampoco deben amontonarse en lugares de paso, ni en locales abiertos.

- Se deben guardar en locales o contenedores que dispongan de mecanismos de cierre que garanticen su seguridad.

A este respecto, debemos destacar muy especialmente la necesidad de que los documentos se almacenen debidamente protegidos, para evitar que se aprovechen para reciclado, para escribir por detrás, hacer cuadernos de notas o simplemente que alguien no autorizado acceda a la información que los mismos pudieran contener.

Con respecto al tema de los contenedores, existe la posibilidad de utilizar unos contenedores especiales (los hay de diferentes capacidades) con abertura como los buzones y que permiten echar papel, pero de los que no se pueden extraer documentos, cuya llave suele estar en posesión de la empresa externa que los recoge y sustituye para proceder a la destrucción de los documentos.

En segundo lugar, se prevén una serie de recomendaciones para el caso de que la documentación sea objeto de transporte hacia un lugar distinto donde va a llevarse a cabo su destrucción. Señalar, en este sentido, que el artículo 92.3 del nuevo Real Decreto 1720/2007, relativo a la gestión de documentos, establece que *"en el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte"*. Asimismo, su artículo 114 señala que *"siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado"*. Las previsiones del Documento sobre *Recomendaciones para la destrucción física de documentos de archivo en papel de la Administración General del Estado* encajan perfectamente con esta filosofía, señalando lo siguiente:

- El transporte, en su caso, hasta el lugar donde vaya a llevarse a cabo la destrucción debe garantizar que durante el traslado no se produzcan sustracciones, pérdidas ni filtraciones de información.

- Todas las operaciones de recogida, carga y descarga de los documentos o sus contenedores, así como la conducción de los vehículos que los transportan, deben ser realizadas por personal debidamente autorizado y fácilmente identificable.

- Los documentos deben ser llevados directamente al lugar donde esté prevista la destrucción, en vehículos cerrados que recorran el trayecto sin paradas ni interrupciones.

Añadir a este respecto únicamente que, en algunos casos, el transportista no tiene llave de los contenedores que transporta, a fin de asegurar totalmente la confidencialidad de los documentos durante su traslado.

Seguidamente, el Documento se refiere a lo que sería el proceso de destrucción de la documentación propiamente dicho. Este quizá sea el apartado más interesante del mismo. A este respecto, se establecen las siguientes recomendaciones:

- La destrucción debe ser inmediata y hacer imposible la reconstrucción de los documentos y la recuperación de cualquier información contenida en ellos.

- Los documentos no deben depositarse en contenedores, al descubierto ni en paquetes, cajas o legajos, junto con el resto de los desechos. Siguen siendo perfectamente legibles y permanecen en la vía pública durante un tiempo indeterminado, al alcance de cualquier persona.

- Entregarlos o venderlos como papel usado para su reciclaje, sin destrucción previa, tampoco es un método seguro. El receptor o comprador de papel usado normalmente realizará una selección, descartando lo que considere inútil, sin que el responsable de los documentos sepa cual será el destino del papel que no se considere apto para el reciclaje. Por otra parte, puede almacenar intacto, durante un tiempo indeterminado y sin ninguna medida de seguridad, el material reciclable en espera de reunir una cantidad suficiente de papel de un mismo tipo o color.

- El enterramiento de los documentos no supone la desaparición inmediata de la información. Antes al contrario, se ha comprobado que el papel se conserva más tiempo enterrado que si se dejase al aire libre.

- La incineración acaba con la información, pero resulta peligroso para el entorno, puede perjudicar al medio ambiente e impide el reciclaje.

- El método más adecuado es la trituración mediante corte en tiras o cruzado, previa a la venta para reciclaje. El papel se hace tiras o partículas, cuyo tamaño se elegirá en función del nivel de protección requerido por la información contenida en los documentos a destruir.

Llegados a este punto haremos una pequeña parada para matizar el tema de la trituración de documentos. La mayor parte de los proveedores de máquinas destructoras de papel o de servicios de destrucción de documentos utilizan la norma DIN 32757 como referencia para indicar los niveles de seguridad ofrecidos. Dicha norma establece cinco grados de seguridad y determina el tamaño máximo de las tiras o partículas en función de ese nivel:

- *Nivel 1:* Tiras de un máximo de 12 mm de ancho. Documentos generales que deben hacerse ilegibles.

- *Nivel 2:* Tiras de un máximo de 6 mm de ancho. Documentos internos que deben hacerse ilegibles.

- *Nivel 3:* Tiras de un máximo de 2 mm. de ancho / Partículas de un máximo de 4 x 80 mm. Documentos confidenciales.

- *Nivel 4:* Partículas de un máximo de 2 x 15 mm. Documentos de importancia vital para la organización que deben mantenerse en secreto.

- *Nivel 5:* Partículas de un máximo de 0,8 x 12 mm. Documentos clasificados, para los que rigen exigencias de seguridad muy elevadas.

Como puede apreciarse, los niveles que establece la norma DIN 32757 no se corresponden con los niveles ni con las categorías de datos que establece nuestra vigente normativa sobre protección de datos de carácter personal. Entendemos que lo más interesante sería hacer a este respecto una equiparación de niveles, que podría ser, a modo de ejemplo, de la siguiente manera:

- *Nivel básico Real Decreto 1720/2007:* Niveles 1 y 2 norma DIN 32757.

- *Niveles medio Real Decreto 1720/2007:* Nivel 3 norma DIN 32757.

- *Nivel alto Real Decreto 1720/2007:* Niveles 4 y 5 norma DIN 32757.

Una matización más al respecto: puestos a elegir, entendemos que es mejor la destrucción en partículas que en tiras, ya que si estamos ante hojas apaisadas (tipo Excel, por ejemplo) las tiras se podrían leer e incluso, con cierta dosis de paciencia, alguien podría llegar a reconstruir el documento.

Finalmente, el Documento sobre *Recomendaciones para la destrucción física de documentos de archivo en papel de la Administración General del Estado* hace referencia al tema de las garantías en caso de que se contrate una empresa especializada en servicios de destrucción de documentos (opción que puede resultar aconsejable en función del volumen de documentación y de los medios técnicos exigidos). En este sentido, la empresa prestadora del servicio se debe comprometer a:

- Garantizar la destrucción de los documentos en sus instalaciones y con medios propios, sin subcontratos que conlleven el manejo de los documentos por parte de otras empresas sin conocimiento del responsable de los documentos.

- Permitir que, siempre que lo estime conveniente, un representante del responsable de los documentos presencie la destrucción de los documentos y compruebe las condiciones en que se realiza y los resultados.

- Certificar la destrucción de los documentos, dejando constancia del momento y de la forma de destrucción.

A este respecto, nos gustaría matizar lo siguiente: el centro de enseñanza ha de ser plenamente consciente de que, al externalizar la destrucción de la documentación, está facilitando una gran cantidad de información concerniente a personas físicas identificadas o identificables a un tercero con personalidad jurídica distinta para que pueda prestarle el citado servicio, debiendo firmarse, en su consecuencia, un contrato con el mismo en el sentido del artículo 12 de la LOPD. En dicho contrato se deberán recoger, como mínimo, las instrucciones fijadas por el responsable del fichero para la prestación del servicio, la finalidad del tratamiento (la destrucción física de la documentación) y la imposibilidad de la comunicación de los datos a terceros distintos del prestador. Asimismo, en el contrato se habrán de estipular las medidas de seguridad que el tercero deberá implantar para la prestación del servicio.

En referencia a la posibilidad de que un representante del responsable de los documentos pueda presenciar personalmente el proceso de destrucción, señalar que algunas empresas especializadas suelen entregar un vídeo del mismo al responsable. Si bien entendemos que la idea del vídeo es positiva, es interesante que cuanto menos en alguna ocasión esté presente un representante del centro cuya documentación está siendo objeto de destrucción, a fin de presenciar el proceso *in situ*.

Asimismo, resaltar la importancia de exigir a la empresa prestadora del servicio un certificado de garantía de destrucción de la documentación que acredite la completa eliminación de la misma. Incluso sería interesante que en el contrato que se firme con la empresa prestadora del servicio se especificase el tamaño máximo de las partículas resultado de la trituración, en milímetros.

Para finalizar, un último apunte sobre el proceso de destrucción de la documentación: se puede sopesar la posibilidad de que a lo largo del citado proceso se incorporen algunos controles adicionales que puedan mejorar la seguridad del mismo, tales como los siguientes:

- Designar un Responsable de Seguridad que asuma formalmente las funciones de coordinar y controlar el proceso de destrucción de los documentos, al menos para el caso de que se trate de documentación que contenga datos de nivel medio o alto. Esta persona podría ser también quien asistiese de manera presencial a los procesos de destrucción de la documentación por parte de la empresa externa, en su caso.

- Diseñar un procedimiento de gestión y resolución de incidencias que puedan surgir durante el proceso de destrucción de los documentos (por ejemplo, el depósito de documentación que vaya a ser eliminada en un lugar que no esté debidamente protegido).

CAPÍTULO V

RECOMENDACIONES PARA EL CORRECTO TRATAMIENTO DE LAS IMÁGENES DEL ALUMNADO POR LOS CENTROS DE ENSEÑANZA

1. Introducción

La informatización de los centros docentes lleva intrínsecamente aparejada la aparición de nuevas formas de tratamiento de las imágenes del alumnado: la creación de páginas web con información sobre los centros en los cuales se incluyen imágenes del alumnado o la instalación de cámaras de videovigilancia en los mismos, se unen ahora a otra serie de cuestiones que pueden afectar a la intimidad del alumnado, como la confidencialidad de su expediente académico o de los informes elaborados por los orientadores y orientadoras de los centros.

Por encima de cualquier otra consideración, los centros de enseñanza deben ser plenamente conscientes de que el alumnado es titular de dos derechos fundamentales que hay que respetar: el derecho a su intimidad y el derecho a la protección de sus datos de carácter personal. Ambos derechos están regulados por la 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 y la LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, respectivamente.

2. Uso de sistemas de cámaras y videocámaras en el centro de enseñanza

2.1. Exposición general de la cuestión

De un tiempo a esta parte, un gran número de centros educativos han optado por instalar cámaras de videovigilancia en el interior de los mismos (puertas de acceso, patios, pasillos, etc.). Esta medida ha venido acompañada, como cabía esperar, de una cierta polémica, ya que parte de la comunidad educativa entiende que podría afectar a algunos de sus derechos fundamentales constitucionalmente reconocidos (intimidad, honor, propia imagen). De igual manera, también podría afectar a su derecho a la protección de datos de carácter personal reconocido en la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

En lo referente a la posible vulneración del derecho a la protección de datos de los miembros de la comunidad educativa como consecuencia de la instalación de cámaras de videovigilancia, conviene aquí recordar que, conforme a lo establecido en el artículo 2.a) de la 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, se entiende por dato personal *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"* .

Atendiendo a la citada definición, que considera dato de carácter personal *"toda información sobre una persona física identificada o identificable"*, las imágenes grabadas en los centros educativos se ajustarán a este concepto siempre que permitan la identificación de las personas que aparecen en dichas imágenes (alumnado, profesorado, personal de administración y servicios, etc.). La propia Directiva 95/46/CE en su Considerando 14 lo afirma expresamente al señalar:

"(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos".

El 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, también considera la imagen como un dato de carácter personal, al definir como tal *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"* (art. 5.1.f)).

Partiendo de esta premisa, contamos con cuatro importantes documentos de referencia:

- El DICTAMEN 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara del Grupo del artículo 29 sobre protección de datos, adoptado el 11 de febrero de 2004, fruto de los trabajos preparatorios plasmados en el DOCUMENTO DE TRABAJO (WP 67), relativo al tratamiento de datos personales mediante vigilancia por videocámara, del Grupo del artículo 29 sobre protección de datos, adoptado el 25 de noviembre de 2002.

- La INSTRUCCIÓN 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, cuyo ámbito de aplicación es el tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

- La INSTRUCCIÓN 1/1996, de 1 de marzo, de la Agencia Española de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios, cuyo objeto

de regulación son los datos de carácter personal tratados de forma automatizada que son recabados por los servicios de seguridad con la finalidad de controlar el acceso a los edificios públicos y privados, así como a establecimientos, espectáculos, certámenes y convenciones, debiendo entenderse comprendidos los datos constituidos por sonido e imagen, como los de vigilancia por videocámara.

- El DOCUMENTO DE TRABAJO 1/08, sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios) del Grupo del artículo 29 sobre protección de datos, adoptado el 18 de febrero de 2008.

Estos cuatro documentos giran en torno a un mismo concepto: la consideración de la imagen relativa a una persona identificada o identificable como un dato de carácter personal lleva aparejada la indisoluble aplicación de los principios de protección de datos establecidos en la Directiva 95/46/CE y en la Ley Orgánica 15/1999, que es transposición de la misma. En este sentido, la propia Instrucción 1/2006 señala expresamente que *"la seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático"*.

Asimismo, los citados textos inciden con fuerza en la necesidad de que la instalación de cámaras de videovigilancia sea una medida proporcional en relación con el bien jurídico que se quiere proteger (no olvidemos que estamos ante la limitación de un derecho fundamental).

En el ámbito concreto de la Comunidad Autónoma de Madrid, cabe citar la Instrucción 1/2007, de 16 de mayo, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid, elaborada a partir de las reuniones de trabajo mantenidas con diferentes sectores de las Administraciones Públicas madrileñas. En este sentido, los Centros Educativos y la propia Administración Educativa informaron a la Agencia de sus experiencias e inquietudes en el marco de una reunión específicamente programada a dicho fin, que contó con la presencia de los Directores y Jefes de Estudio de distintos Centros Públicos de educación primaria y secundaria de la Comunidad de Madrid.

Dicha Instrucción establece que deberán implantarse unas medidas de seguridad reforzadas cuando se realicen tratamientos de imágenes realizados mediante sistemas de cámaras o videocámaras que, de manera directa y específica, se dirijan a la captación y tratamiento de imágenes de personas menores de edad (por ejemplo, imágenes del alumnado de un centro de enseñanza).

Si bien la citada Instrucción no es directamente aplicable a los centros de enseñanza de la Junta de Andalucía sí que es profundamente reveladora de la trascendencia de adoptar las garantías adecuadas en relación al tratamiento de las imágenes del alumnado.

2.2. Proporcionalidad de la medida

El Dictamen 4/2004 del Grupo del artículo 29 sobre protección de datos señala expresamente que *“el circuito cerrado de televisión y otros sistemas similares de vigilancia por videocámara sólo podrán utilizarse con carácter subsidiario, es decir: con fines que realmente justifiquen el recurso a tales sistemas”*.

En idéntico sentido se manifiesta la Instrucción 1/2006, la cual establece que *“en relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación*

deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales". En consecuencia, *"el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo"*.

Siguiendo esta línea argumental, la Instrucción 1/2006 recuerda que *"para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"*.

Trasladando estas premisas básicas a la problemática concreta de los centros de enseñanza, debemos señalar que la instalación de cámaras de videovigilancia ha de ser, en todo caso, una medida proporcional en relación con la infracción que se pretenda evitar. De tal manera, la instalación de videocámaras no tendría justificación si, por ejemplo, se realiza con la finalidad controlar una infracción menor, como la prohibición de fumar en el centro.

En el caso de que la instalación de cámaras de videovigilancia fuera, por ejemplo, controlar determinados actos como robos y daños materiales, el principio de proporcionalidad recogido en el Dictamen 4/2004 nos indica que *"se pueden utilizar estos sistemas cuando otras medidas de prevención, protección y seguridad, de naturaleza física o lógica, que no requieran captación de imágenes (por ejemplo, la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de seguridad, sistemas combinados de alarma, sistemas mejores y más*

potentes de alumbrado nocturno en las calles, etc.) resulten claramente insuficientes o inaplicables en relación con los fines legítimos mencionados anteriormente". Por lo tanto, con anterioridad a la instalación en el centro de enseñanza de cámaras de videovigilancia debería procederse a la puesta en práctica de otra serie de medidas tendentes a evitar los actos citados que no supongan la limitación de derechos fundamentales de los miembros de la comunidad educativa y sólo en el caso de que éstas fracasen sopesar el sistema de videovigilancia como último recurso.

En este último sentido, el art. 4.2 de la Instrucción 1/2006 establece que *"sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal"*.

Para finalizar, debemos citar el Decreto 19/2007, de 23 de enero, por el que se adoptan medidas para la promoción de la Cultura de Paz y la Mejora de la Convivencia en los Centros Educativos sostenidos con fondos públicos, basado en el principio de intervención preventiva, a través de la puesta en marcha de medidas y actuaciones que favorezcan la mejora del ambiente socioeducativo de los centros, las prácticas educativas y la resolución pacífica de los conflictos.

No obstante lo anterior, el art. 3.2.c) del citado Decreto establece que, para la consecución de los objetivos del mismo, se deberá *"Dotar a los centros educativos de los recursos que les permitan mejorar la seguridad de las personas que trabajan en ellos, así como de sus instalaciones"*.

Ahora bien, los centros de enseñanza han ser conscientes de que no debe hacerse un uso masivo de las cámaras de videovigilancia como una medida habitual, debiendo atenderse siempre a las circunstancias particulares y concretas de cada caso en orden a determinar si la medida a adoptar supera o no el correspondiente juicio de proporcionalidad.

2.3. Aplicación de los principios de protección de datos conforme a lo establecido en la Instrucción 1/2006

En el presente apartado, nos centraremos en la aplicación de los principios que vertebran la normativa sobre protección de datos de carácter personal en base a lo establecido en la INSTRUCCIÓN 1/2006, aplicable al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

- *Principio de información*

En este sentido, el art. 3 de la Instrucción 1/2006, que lleva por rúbrica *"Información"*, establece lo que a continuación se detalla:

"Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y
b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999".

El contenido y el diseño del distintivo informativo indicado en el apartado a) del art. 3 debe ajustarse a lo previsto en el apartado 1 del Anexo de la Instrucción 1/2006 (ver ANEXO II de la presente Guía).

En lo referente a los impresos a que hace referencia el apartado b) del art. 3, la Agencia Española de Protección de Datos también ha diseñado el modelo correspondiente, del cual facilitamos la versión destinada a las Administraciones Públicas, entre las cuales se englobarían los centros de enseñanza públicos (ver ANEXO II de la presente Guía).

- *Principio del consentimiento*

Conforme a lo establecido en el art. 2.1 de la Instrucción 1/2006, *"sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal"*.

La postura de la Agencia en este sentido es que debe existir la necesidad de legitimación para que el tratamiento de los datos de carácter personal sea lícito. Esto supone por tanto que o se obtiene el consentimiento de cada uno de los interesados o se cumplen los requisitos que la legislación en la materia establecen para que el tratamiento sea legítimo. La AEPD considera que el tratamiento de imágenes se encuentra amparado en el artículo 5.1.e) de la Ley de Seguridad Privada. De este modo, dado que la Ley permite la instalación y mantenimiento de equipos de seguridad privados legitima a quienes adquieran de estos dispositivos para tratar los datos personales derivados de la captación de las imágenes, siendo dicho tratamiento conforme a lo previsto en la LOPD. Véase El Informe Jurídico 0650/2009 de la AEPD.

- *Principio de calidad de los datos*

A este respecto, el art. 4.1 de la Instrucción 1/2006 señala que *"de conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras"*.

Asimismo, los datos deberán ser cancelados *"en el plazo máximo de un mes desde su captación"* (art. 6 Instrucción 1/2006).

- *Principio de seguridad de los datos*

En este sentido, el art. 9 de la Instrucción 1/2006 establece lo siguiente:

"El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior".

2.4. Aplicación de los principios de protección de datos conforme a lo establecido en la Instrucción 1/1996

Como hemos señalado anteriormente, el objeto de regulación de la Instrucción 1/1996 son los datos de carácter personal tratados de forma automatizada que son recabados por los servicios de seguridad con la finalidad de controlar el acceso a los edificios públicos y privados. En el presente apartado, iremos desgranando cada uno de los principios de la normativa sobre protección en base a lo establecido en la citada Instrucción.

- *Principio de información*

A este respecto, la Instrucción 1/1996 señala que la recogida de las imágenes *"deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992* (entiéndase esta mención hecha ahora a la Ley Orgánica 15/1999, que derogó a la antigua LORTAD)*, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de los datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero"* (Norma Tercera).

Con el objeto de que los centros de enseñanza de la Junta de Andalucía cumplan correctamente con lo establecido en la Norma Tercera de la

Instrucción 1/1996, hemos preparado un modelo orientativo de aviso informativo que deberá ubicarse a la entrada de todos aquellos centros que dispongan de un sistema de cámaras o videocámaras con la finalidad de controlar el acceso al mismo (ver ANEXO II de la presente Guía).

- *Principio del consentimiento*

La Norma Cuarta de la Instrucción 1/1996 establece que las imágenes no podrán ser objeto de cesión *"fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado".*

- *Principio de calidad de los datos*

En lo tocante a este particular, las Normas Cuarta y Quinta de la Instrucción 1/1996 establecen *"los datos personales así obtenidos no podrán ser utilizados para otros fines"* y *"deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados"*.

- *Principio de seguridad de los datos*

Finalmente, la Norma Sexta de la Instrucción 1/1996 señala que *"el responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines"*.

2.5. Medidas de seguridad

Los ficheros de imágenes captadas por sistemas de videovigilancia con fines de seguridad deberán adoptar medidas de seguridad de nivel básico, en los términos previstos en los artículos 81.1 y 89 a 94 del Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999.

2.6. Observaciones realizadas por el Grupo del artículo 29 sobre protección de datos en su Documento de trabajo 1/08

Llegados a este punto, nos gustaría hacer referencia a las observaciones realizadas por el Grupo del artículo 29 sobre protección de datos en su Documento de trabajo 1/08, sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios), adoptado el 18 de febrero de 2008, en referencia a la utilización de circuítos cerrados de televisión (CCTV) en los centros docentes:

"Existe una tendencia creciente a usar circuítos cerrados de televisión (CCTV) en los colegios por motivos de seguridad. No existe una solución válida recomendada para todos los aspectos de la vida escolar y para todas las zonas de los colegios.

La capacidad del circuíto cerrado de televisión (CCTV) para afectar a las libertades personales supone que su instalación en los colegios exige un cuidado especial. Esto supone que sólo debería instalarse cuando sea necesario y si no está disponible otro medio menos intrusivo de lograr el mismo objetivo. La decisión de instalar un circuíto cerrado de televisión (CCTV) deberá estar precedida de un debate exhaustivo entre los profesores, los progenitores y los representantes de los alumnos, teniendo en cuenta los objetivos indicados para la instalación y la adecuación de los sistemas propuestos.

Existen lugares donde la seguridad es de la mayor importancia, por lo que puede justificarse más fácilmente la instalación de CCTV, por ejemplo, en las entradas y salidas de los colegios, así como otros lugares donde circulan las personas (no sólo la población del colegio, sino también personas que visitan las instalaciones escolares por el motivo que sea).

La elección de la ubicación de las cámaras de CCTV deberá ser siempre pertinente, adecuada y no excesiva en relación con el objeto del tratamiento. Por ejemplo, en algunos países, el uso de cámaras de CCTV fuera del horario escolar se consideró adecuado en relación con los principios de protección de datos.

Por otro lado, en la mayoría de las demás partes del colegio, el derecho a la intimidad de los alumnos (así como el de los profesores y otros trabajadores del colegio) y la libertad esencial a la enseñanza, prevalecen sobre la necesidad de vigilancia por CCTV permanente.

Éste es especialmente el caso en las aulas, donde la vigilancia por video puede interferir no sólo en la libertad de los alumnos de aprender y expresarse, sino también en la libertad de enseñar. Lo mismo se aplica a las zonas de ocio, gimnasios y vestuarios, donde la vigilancia puede interferir con el derecho a la intimidad.

Estas observaciones también se basan en el derecho al desarrollo de la personalidad, que poseen todos los niños. De hecho, la concepción en desarrollo de su propia libertad puede verse comprometida si asumen desde una edad temprana que es normal estar vigilado por CCTV. Esto es aún más cierto si se utilizan webcams o dispositivos similares para la vigilancia remota de los niños durante sus horas de colegio.

En cualquier caso en que esté justificado el uso de CCTV, los niños, el resto de la población del colegio y los representantes deberán estar informados de la existencia de la vigilancia, del responsable del tratamiento y de sus objetivos. La información dirigida a los niños deberá ser adecuada a su nivel de entendimiento.

Las autoridades escolares deberán revisar regularmente la justificación y la pertinencia del sistema de CCTV para decidir si debe mantenerse o no.

Los representantes de los niños deberán estar informados en consecuencia."

3. Publicación de imágenes del alumnado en la página web del centro de enseñanza

La difusión de las Tecnologías de la Información y las Comunicaciones (TICs) entre los centros de enseñanza ha propiciado que muchos de ellos dispongan de su propia página web, en las cuales se suele verter nutrida información acerca del mismo, incluyendo en ocasiones imágenes del alumnado del centro en momentos distintos de su actividad escolar.

En este sentido, los centros de enseñanza deben ser plenamente conscientes de la necesidad de contar con el consentimiento previo e informado del alumno, la alumna o el padre, la madre o de su representante legal (en el caso de que aquél no reúna las condiciones de madurez suficientes) a la hora de llevar a cabo actividades de este tipo que pueden afectar a su intimidad (entendida ésta en un sentido amplio).

A este respecto, son dignos de mención dos casos acaecidos en Cataluña y en la Comunidad de Madrid. En el primero de los casos, un grupo de antiguos alumnos de un colegio de Reus (Tarragona) iniciaron una campaña de disconformidad con la inclusión de imágenes suyas en la página web del centro aludiendo al derecho a preservar su intimidad. Algunos meses después, el departamento de Ensenyament de la Generalitat decidió adoptar una resolución en virtud de la cual los centros educativos de Cataluña no pueden mostrar ninguna foto del alumnado en sus páginas web sin contar con el consentimiento previo de sus padres, madres o representantes legales, ofreciendo incluso a los centros un modelo con el cual recoger el consentimiento para tal finalidad. La aprobación de dicha resolución tuvo su fundamento legal en el reconocimiento del derecho fundamental a la propia imagen en el art. 18.1 de la Constitución, desarrollado a través de la 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.

En este sentido, la Ley Orgánica 1/1982, establece que *"no se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por la Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso"* (art. 2.2 L.O. 1/1982).

Asimismo, señala que *"el consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil"* (art. 3.1 L.O. 1/1982), lo cual es un condicionante que también debe ser tenido muy en cuenta por los centros de enseñanza.

En el segundo de los casos citados, el padre de un alumno de un colegio público de la Comunidad de Madrid compareció ante el Defensor del Menor manifestando su preocupación por la aparición de la imagen del alumnado en la página web del centro, sin que mediara autorización de sus padres.

Al igual que en el caso anterior, se tomó en consideración el derecho fundamental a la propia imagen regulado a través de la Ley Orgánica 1/1982. De acuerdo con lo establecido en el art. 2.2 de la citada Ley, la facultad de disponer de la imagen de una persona requiere del consentimiento expreso de su titular. El Defensor del Menor entendió aquí que, aún admitiendo un interés educativo o cultural, ese interés no parecía tener un carácter tan relevante que le hiciera prevalecer sobre el derecho del alumnado a su propia imagen.

En base a lo anteriormente expuesto, el Defensor del Menor formuló una Recomendación a la dirección del centro para que se adoptaran las medidas oportunas dirigidas a evitar en el futuro la difusión de la imagen de los y las menores de edad matriculados en el mismo, sin recabar previamente el consentimiento del o la propio/a menor titular del derecho, si tuviera suficiente madurez o, en caso contrario, de su padre, madre o representante legal, con conocimiento previo del Ministerio Fiscal y, así mismo, se llevasen a cabo las acciones oportunas para subsanar la omisión de tal requisito, en la difusión que se estaba produciendo a través de la

página web del centro. Dicha resolución fue plenamente aceptada por el centro educativo.

No obstante todo lo anterior, la 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 no es la única norma que protege la imagen del o la menor, ya que ésta es también un dato de carácter personal digno de protección conforme a lo establecido en la Ley Orgánica 15/1999 (nuestra tantas veces citada LOPD).

De tal manera, la Sentencia de la Audiencia Nacional de 24-01-2003, relativa al tratamiento de datos de carácter personal a través de imágenes captadas por una webcam y su transmisión a través de Internet, declaró en su Fundamento de Derecho Segundo que *"el artículo 3.a) de la Ley Orgánica 15/1999 ofrece una definición amplia de "datos de carácter personal" pues refiere este concepto a cualquier información concerniente a personas físicas identificadas o identificables. Por su parte el artículo 1.4 del Real Decreto 1332/1994, de 20 de junio -que, aunque dictado en desarrollo de la ya derogada Ley Orgánica 5/1992, continua estando en vigor de conformidad con la disposición transitoria tercera de la Ley Orgánica 15/1999*[1]*- considera datos de carácter personal a toda información numérica, alfabética gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable"*, añadiendo expresamente que, aún con todo, *"la formulación del artículo 3.a) de la LOPD es de tal amplitud que aunque no hubiese existido la mencionada especificación reglamentaria habría que considerar incluidos en aquélla los datos consistentes en imágenes"*.

En la misma Sentencia, la Audiencia Nacional señaló que *"no cabe duda de que la emisión de las imágenes a través de Internet conlleva su cesión o la puesta de las mismas a disposición de un destinatario múltiple e indeterminado"* (Fundamento de Derecho Tercero). Precisión perfectamente aplicable a la publicación de imágenes del alumnado a través de la página web de un centro de enseñanza.

1 Actualmente no es así, puesto que el Reglamento de Desarrollo de la LOPD (RD 1720/2007) ha derogado el Real Decreto 1332/1994, si bien, en su artículo 5.1.f), define dato de carácter personal de un modo casi coincidente con el establecido en dicho Real Decreto: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Por último, la Sentencia de la Audiencia Nacional de 24-01-2003, precisó en su Fundamento de Derecho Cuarto que, si bien la Ley Orgánica 15/1999 no requiere que el consentimiento para el tratamiento de las imágenes se preste por escrito o con formalidades determinadas, sí exige que el consentimiento de los afectados sea *"inequívoco"*. Es decir, para proceder a la publicación de imágenes de los alumnos y alumnas a través de la página web de un centro de enseñanza es necesario el consentimiento previo e inequívoco de cada uno de ellos (o de sus padres, madres o representantes legales, en función de sus condiciones de madurez).

Asimismo, las imágenes publicadas no deben ser contrarias al honor del alumnado. Por tanto, las fotografías que vayan a ser objeto de publicación en la Red han de realizarse en un entorno y con la vestimenta adecuadas a la finalidad legítima para la cual se van a utilizar, evitando cualquier otro uso desviado o inadecuado de las mismas. No podemos olvidar que publicar las imágenes del alumnado en Internet supone, como hemos indicado, su puesta a disposición a un destinatario múltiple e indeterminado y la salvaguarda de los y las menores ha de estar por encima de cualquier otro condicionante.

Como es obvio, idénticas consideraciones deberán tenerse en cuenta a la hora de hacer pública en la Red no ya sólo sus imágenes, sino cualquier otro tipo de información concerniente al alumnado del centro educativo (nombre y apellidos, centro en el que estudia, curso, edad, calificaciones, etc.), ya que ello implicaría su cesión a un destinatario múltiple e indeterminado.

Sobre este particular, el reciente Documento de Trabajo 1/08, sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios) del Grupo del artículo 29 sobre protección de datos, adoptado el 18 de febrero de 2008, señala lo siguiente:

"Sitios web de los colegios.

Un número creciente de colegios crean sitios web dirigidos a los alumnos/estudiantes y sus familias, y dichos sitios web se convierten en la herramienta principal para las comunicaciones externas. Los colegios deben ser conscientes de que divulgar información personal justifica un

cumplimiento más riguroso de los principios fundamentales de protección de datos, en concreto, la proporcionalidad y minimización de los datos; adicionalmente, se recomienda la puesta en marcha de mecanismos de acceso restringido con vistas a proteger la información personal en cuestión (es decir, conexión con nombre de usuario y contraseña).”

“Fotos de los niños.

Con frecuencia, los colegios están tentados de publicar (en la prensa o en internet) fotos de sus alumnos. Debe prestarse especial atención a la publicación por parte de los colegios de fotos de sus alumnos en Internet. Siempre debe hacerse una evaluación del tipo de foto, la pertinencia de su publicación y su objetivo. Los niños y sus representantes deben ser conscientes de su publicación y deberá obtenerse el consentimiento previo del representante (o del niño, si ya es maduro).”

La Consejería de Educación de la Junta de Andalucía, consciente de toda esta problemática, ha decidido diseñar modelos orientativos de solicitud del consentimiento para la publicación de imágenes del alumnado en la página web del centro de enseñanza (ver ANEXO II de la presente Guía), así como modelos orientativos de solicitud del consentimiento para la publicación de otro tipo de datos de carácter personal de los alumnos y alumnas en la página web del centro de enseñanza (ver ANEXO I de la presente Guía), que sirvan de utilidad a los centros de enseñanza.

4. Enlaces a la normativa específica sobre tratamiento de imágenes

4.1. Normativa de la Unión Europea

- DICTAMEN 4/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, del Grupo del artículo 29 sobre protección de datos, adoptado el 11 de febrero de 2004. Disponible en el apartado de Protección de Datos del Sitio Web de la Comisión Europea:
  http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_es.pdf

- DOCUMENTO DE TRABAJO 1/08, sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios) del Grupo del artículo 29 sobre protección de datos, adoptado el 18 de febrero de 2008. Disponible en el Sitio Web de la Agencia Española de Protección de Datos:
  https://www.agpd.es/upload/Canal_Documentacion/Internacional/wp_29/menores_es.pdf

- DOCUMENTO DE TRABAJO (WP 67), relativo al tratamiento de datos personales mediante vigilancia por videocámara, del Grupo del artículo 29 sobre protección de datos, adoptado el 25 de noviembre de 2002. Disponible en el apartado de Protección de Datos del Sitio Web de la Agencia Española de Protección de Datos:
  http://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2002/common/pdfs/Documento-de-trabajo-relativo-al-tratamiento-de-datos-personales-mediante-vigilancia-por-videoc-aa-m.pdf

4.2. Normativa nacional

- 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.

http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1982-11196

- INSTRUCCIÓN 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2006-21648

- INSTRUCCIÓN 1/1996, de 1 de marzo, de la Agencia Española de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios. http://www.boe.es/diario_boe/txt.php?id=BOE-A-1996-5697

- Orden de 26 de abril de 2010, por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por la Consejería de Educación en el ámbito de la videovigilancia en centros educativos. (BOJA 91, de 12 de mayo). http://juntadeandalucia.es/boja/boletines/2010/91/d/updf/d20.pdf

CAPÍTULO VI

PREGUNTAS FRECUENTES SOBRE LA APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS CENTROS DE ENSEÑANZA

1. El derecho a la protección de datos

1.1. ¿Qué es el derecho a la protección de datos de carácter personal?

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, consagró el derecho a la protección de datos de carácter personal como un derecho fundamental independiente, desvinculado del derecho a la intimidad, cuyo contenido está integrado por los principios y derechos que se contemplan en la LOPD.

Este derecho autónomo e informador de nuestro texto constitucional se concreta en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a su posesión o uso.

Como consecuencia de lo anterior, todo tratamiento de datos de carácter personal requiere el consentimiento previo e inequívoco del interesado o titular de los mismos, principio legitimador en torno al cual se vertebra la normativa española sobre protección de datos y que permite a la persona ejercer el control efectivo del uso de sus datos por parte de terceros.

2. Inscripción de ficheros

2.1. ¿Quién es el responsable de notificar los ficheros en el Registro General de Protección de Datos en el caso de los centros de enseñanza pública?

En el caso de los centros de enseñanza pública, se plantea la duda de si ha de ser el propio centro de enseñanza o la Consejería de la cual depende quien deba proceder a la adopción de la disposición de carácter general señalada en el art. 20 LOPD y la posterior publicación de la misma en el Boletín Oficial del Estado o Diario oficial correspondiente, así como a la consiguiente notificación de sus ficheros a fin de lograr su inscripción en el Registro General de Protección de Datos.

Dicha cuestión ha sido resuelta por la Agencia Española de Protección de Datos en su Informe Jurídico 143/2004, indicando lo siguiente:

"… la obligación de notificación corresponderá al responsable del fichero, definido por el artículo 3 d) de la Ley Orgánica 15/1999 como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

Para determinar a quién corresponde la obligación de proceder a la adopción de la correspondiente disposición de carácter general y la consiguiente notificación del tratamiento al Registro General del Protección de Datos resulta imprescindible delimitar si el consultante es un órgano incardinado en la Administración Autonómica o si el mismo posee personalidad jurídica independiente de la misma.

En el primer supuesto, el Centro no sería sino un mero usuario del fichero, cuyo responsable sería la Administración educativa autonómica, de forma que la obligación de notificación correspondería a la Consejería de Educación, debiendo hacerse referencia al Centro educativo únicamente como lugar de ubicación del fichero. En caso contrario, el responsable del fichero sería el propio Centro, correspondiendo al mismo la notificación del tratamiento al Registro de esta Agencia."

En este sentido, la Consejería de Educación de la Junta de Andalucía ha creado la ORDEN de 20 de julio de 2006, por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por la Consejería de Educación en el ámbito de los sistemas Séneca y Pasen, publicada en el BOJA núm. 156, de fecha 11 de agosto de 2006.

3. Ámbito de aplicación de la normativa

3.1. Los ficheros de un centro docente concertado, ¿se rigen por lo establecido para los ficheros de titularidad pública o por el contrario les es de aplicación el régimen de ficheros de titularidad privada?

Según lo establecido en el art. 108 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación (en adelante, LOE), los centros docentes se clasifican en públicos y privados. De tal manera, son centros públicos aquellos cuyo titular sea una Administración Pública y son centros privados aquellos cuyo titular sea una persona física o jurídica de carácter privado.

En cuanto a los centros concertados, a efectos de lo establecido en la LOE, debemos entender por tales los centros privados acogidos al régimen de conciertos legalmente establecido (de hecho, la propia Ley Orgánica 2/2006 los denomina *"centros privados concertados"*. La firma de un concierto educativo implica que los centros privados concertados impartan enseñanzas en régimen de gratuidad y la aplicación de similares normas que las dispuestas para los centros públicos en lo que afecta a la admisión de alumnos, órganos de gobierno y participación, así como normas específicas en lo que afecta a la contratación y despido del profesorado.

Por otra parte, el Capítulo I del Título IV de la LOPD, que regula los ficheros de titularidad pública, se refiere expresamente los ficheros de las Administraciones Públicas. Por tanto, en principio, los ficheros de datos de carácter personal tratados en los centros privados concertados deberán acogerse al régimen establecido para los ficheros de titularidad privada (como también se establece en el artículo 5.1.l) del Real Decreto 1720/2007, por el que se aprueba del Reglamento de desarrollo de la LOPD). Ello con independencia de que la prestación del servicio público de la educación se realice también a través de los centros privados concertados (además de los centros públicos).

Con respecto al fichero de personal de los centros privados concertados, hay que tener en cuenta que es la propia Administración quien abona los salarios al personal docente. Ahora bien, dichas remuneraciones son

realizadas en concepto de pago delegado y en nombre de la entidad de carácter privado titular del centro, ya que es esta última quien ostenta la condición de empleador en la relación laboral. Por tanto, el citado fichero deberá regirse, de igual forma, por el régimen establecido para los ficheros de titularidad privada. Señalar, por último, que para poder realizar dichos abonos, el titular del centro debe facilitar a la Administración las nóminas correspondientes, así como sus eventuales modificaciones, debiendo, por ende, informarse de esta comunicación de datos a los interesados o interesadas (el personal docente del centro privado concertado).

3.2. ¿Sería aplicable la LOPD a los informes psicopedagógicos realizados por los orientadores y orientadoras sobre un procesador de textos?

Por lo general, los orientadores y orientadoras no manejan ficheros de datos de carácter personal en el sentido coloquial del término, utilizando como única herramienta informática el procesador de textos para la redacción de informes psicopedagógicos y otros documentos propios del ejercicio de su actividad profesional.

La pregunta que se plantea, pues, es si el conjunto de dichos documentos de texto conformarían un fichero conforme a lo establecido en nuestra LOPD.

En este sentido, debemos señalar que el concepto de fichero, a efectos de lo establecido en la Ley Orgánica 15/1999, parte esencialmente de que exista un conjunto organizado de datos de carácter personal empleado por el Responsable del fichero para el cumplimiento de una finalidad específica: *"Art. 3.b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"*.

En su consecuencia, lo relevante para considerar si estamos en presencia de un fichero será la individualización de los datos que contiene, con independencia de las características del sistema de información dispuesto para su tratamiento y almacenamiento. Por tanto, en principio, un

conjunto de documentos de texto ordenados alfabéticamente en función de los apellidos y nombre del alumnado, creados para la finalidad específica de prestar el servicio de orientación psicopedagógica por parte del centro, podría tener la consideración de fichero a los efectos de la Ley Orgánica 15/1999.

Un aspecto muy importante a tener en cuenta es que, en tanto en cuanto los documentos en cuestión contengan datos psicológicos, considerados como datos de salud por la Agencia Española de Protección de Datos, deberán implementarse las medidas de seguridad contempladas en el Real Decreto 1720/2007 para los ficheros que contengan datos de carácter personal catalogados de nivel alto. En este sentido, plantea especiales dificultades el establecimiento del *"Registro de accesos"* contemplado en el art. 103 del citado Real Decreto.

En este sentido, a juicio de la AEPD, *"el aspecto esencial a tener en consideración en estos casos será el que la información almacenada en el registro de accesos permita identificar inequívocamente qué persona ha tenido acceso a qué información contenida en el fichero en cada momento, a fin de que, en caso de ser necesario reconstruir cuándo y cómo se produjo una determinada revelación de un dato, sea posible identificar la persona que pudo conocerlo en ese momento concreto.*

*Por ello, dependerá de las aplicaciones informáticas con que cuente el responsable del fichero dar una u otra solución, de forma que, en caso de que ante la cuestión de quién conoció un determinado dato en un concreto momento, sea posible efectuar esa reconstrucción"***.**

3.3. Si en un centro de enseñanza se realizan encuestas anónimas entre el alumnado y sus familiares para realizar un estudio sobre salud y hábitos alimentarios, ¿sería aplicable la normativa sobre protección de datos de carácter personal al supuesto concreto?

No. En este sentido, el art. 2.1 LOPD señala que *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso*

posterior de estos datos por los sectores público y privado"; definiéndose el concepto de dato de carácter personal en el artículo 3.a) de la citada LOPD como *"Cualquier información concerniente a personas físicas identificadas o identificables"*.

De igual manera, la Audiencia Nacional, en su sentencia de 08/03/2002, ha señalado que *"no hay datos de carácter personal, y por tanto no es posible aplicar la Ley de Protección de Datos a los llamados "datos disociados" y así el mismo artículo 3 de la Ley, pero en su apartado f), define como "Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable"*.

Y añade la citada sentencia: *"Procedimiento de disociación que consiste en eliminar la conexión entre el dato y la persona, en "despersonalizar" el dato, actuando como barrera que impide la identificación y entrañando en definitiva un elemento protector de la intimidad o privacidad del afectado.*

Sin embargo, para que exista dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados, tal y como se desprende del mencionado artículo 3 de la Ley, en sus apartados a) y f) y también del Considerando 26 de la invocada Directiva 95/46/CE que expresamente señala que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al art. 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado".

En su consecuencia, dado que las encuestas realizadas en el centro de enseñanza son anónimas, en principio, no sería aplicable la normativa

vigente sobre protección de datos de carácter personal, al no ser posible identificar a través de las mismas (salvo que se recurriese a medios desproporcionados, como la utilización de los servicios especializados de un grafólogo) a las personas que las han cumplimentado y, por tanto, relacionarlas con sus hábitos alimentarios.

3.4. En un centro de enseñanza disponen de cámaras de vigilancia, si bien sólo se utilizan para el visionado en tiempo real de las imágenes captadas, sin proceder a su grabación o conservación. ¿Sería aplicable en este supuesto la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras?

Sí. En este sentido, el artículo 1 apartado 1 de la Instrucción 1/2006 comprende, dentro de su ámbito objetivo de aplicación, *"la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas"*.

Por tanto, la citada Instrucción es aplicable a cualquier centro de enseñanza que disponga de cámaras, videocámaras o cualquier otro medio técnico análogo o sistema que permita el visionado en tiempo real de las imágenes del alumnado, personal docente, etc. . Otra cosa es que no exista la obligación de inscribir el fichero de videovigilancia, puesto que, tal como dice la Instrucción en su artículo 7: *"2. No se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real".*

4. Principio del consentimiento

4.1. ¿A partir de qué edad puede una persona consentir sobre el tratamiento de sus datos?

Todo tratamiento de datos de carácter personal requiere el consentimiento previo e inequívoco del interesado, interesada o titular de los mismos, principio legitimador en torno al cual se vertebra la normativa española sobre protección de datos y que permite a la persona ejercer el control efectivo del uso de sus datos por parte de terceros.

Ahora bien, en el ámbito educativo esta cuestión se complica, ya que en la gran mayoría de los casos estamos hablando de personas menores de edad. Surge, por tanto, la inevitable pregunta de si éstas gozan o no de la capacidad jurídica suficiente para consentir sobre el tratamiento de sus datos.

La Agencia Española de Protección de Datos señala, respecto al consentimiento de los menores de edad, que deben diferenciarse dos supuestos básicos:

1. Los y las mayores de catorce años, a los que la Ley atribuye capacidad para la realización de determinados negocios jurídicos.

2. El consentimiento que pudieran dar los y las menores de dicha edad.

Respecto de los y las mayores de catorce años, la AEPD recuerda que el artículo 162.1º del Código Civil exceptúa de la representación legal del titular de la patria potestad a *"los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo"*.

De tal modo, la AEPD entiende que las personas mayores de catorce años reúnen las condiciones suficientes de madurez para prestar

su consentimiento al tratamiento de los datos, toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los y las mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos/as determinados actos de la vida civil (adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, capacidad para testar, etc.).

Respecto de los y las restantes menores de edad, la AEPD entiende que no puede ofrecerse una solución claramente favorable a la posibilidad de que por los/las mismos/as pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162.1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez.

En consecuencia, será necesario recabar el consentimiento de los y las menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley, recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales.

El reciente 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 incorpora, de manera definitiva, el criterio interpretativo de la Agencia Española de Protección de Datos plasmado en su Memoria 2000, regulando, asimismo, otros aspectos de importancia en referencia a la captación de datos de menores:

"Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales."

De tal manera, el apartado 1 del citado artículo 13 sitúa definitivamente la barrera del consentimiento para el tratamiento de los datos de las personas menores de edad en los catorce años, señalando que *"podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela"* y que *"en el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores"*.

4.2. ¿Puede un centro de enseñanza publicar en su página web imágenes del alumnado sin su consentimiento previo?

No. En este sentido, conviene recordar que, conforme a lo establecido en el artículo 2.a) de la Directiva 95/46/CE, se entiende por dato personal *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física,*

fisiológica, psíquica, económica, cultural o social". Atendiendo a la citada definición, que considera dato de carácter personal *"toda información sobre una persona física identificada o identificable"*, las imágenes publicadas en la página web se ajustarán a este concepto siempre que permitan la identificación de los alumnos y alumnas del centro de enseñanza.

Por tanto, de conformidad con lo establecido en los arts. 6.1 y 11.1 de la LOPD, la publicación de las imágenes del alumnado en la página web del centro de enseñanza requerirá el consentimiento previo e inequívoco de los mismos o bien de sus padres, madres o representantes legales, si no reuniesen las condiciones de madurez suficientes.

Asimismo, la 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, establece que *"no se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por la Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso"* (art. 2.2 L.O. 1/1982). De lo cual se infiere que es necesario contar con el consentimiento expreso de los alumnos y alumnas o bien de sus padres, madres o representantes legales, si no reuniesen las condiciones de madurez suficientes, para la publicación de sus imágenes en la página web del centro de enseñanza.

4.3. ¿Puede el alumno o alumna negarse a que sus padres conozcan sus calificaciones?

No. Esta cuestión fue planteada a la Agencia Española de Protección de Datos en 2004, más concretamente si debía prevalecer la voluntad de un alumno de catorce años que no quería que se facilitasen sus calificaciones académicas a sus padres o tutores, sobre la pretensión de éstos de acceder a dicha información, no pudiendo en dicho caso el centro de enseñanza atender la citada solicitud de los padres o tutores. Asunto que la AEPD resolvió en su Informe 466/2004, de la siguiente manera:

"En cuanto a la posibilidad de ceder los datos académicos de los menores a sus padres o tutores sin el consentimiento de dichos menores afectados, ante todo, deberá considerarse que la comunicación de los datos al representante legal supone una cesión de datos de carácter personal, definida por el artículo 3 i) de la Ley como "Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado."

Respecto de las cesiones, el artículo 11.1 prevé taxativamente que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado." Este consentimiento sólo se verá exceptuado en los supuestos contenidos en el artículo 11.2 de la Ley, entre los que se encuentra la posibilidad de que una norma con rango de Ley habilite la cesión.

Pues bien, de acuerdo con lo dispuesto por el artículo 154 del vigente Código Civil:

"Los hijos no emancipados están bajo la potestad del padre y de la madre. La patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad, y comprende los siguientes deberes y facultades:

1. *Velar por ellos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral.*

2. Representarlos y administrar sus bienes (.....)".

En consecuencia, toda vez que la facultad de acceder a la información de carácter académico a la que se refiere la consultante (entre la que se cita la cesión relativa a las calificaciones obtenidas por los menores), se encuentra dentro del marco de los deberes y derechos que corresponden a los padres, inherentes al ejercicio de su patria potestad, cabe concluir que en el supuesto de los hijos no emancipados existe una norma legal habilitante que ampara la cesión de los datos académicos de los menores a sus padres, derivada de lo previsto en el transcrito artículo 154 del Código Civil."

Parece lógico. Obviamente, si los padres del o la menor tienen el deber de educar y procurar una formación integral a sus hijos e hijas difícilmente podrán hacerlo sin tener acceso a sus calificaciones. Con lo cual, la AEPD ha truncado, con buen criterio, el sueño de todo mal o mala estudiante deseoso/a de ocultar los suspensos a sus padres y madres.

4.4. ¿Sería aplicable la excepción al consentimiento del art. 11.2.a) LOPD a aquellos casos en que una norma infralegal autorice la cesión de datos de carácter personal?

No. El art. 11.2.a) LOPD establece que el consentimiento del interesado previo a la comunicación de sus datos no será preciso cuando la cesión está autorizada en una ley. Ahora bien, tal y como ha señalado el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, que consagró el derecho fundamental a la protección de datos de carácter personal, la posibilidad *"de que una norma reglamentaria pueda autorizar la cesión de datos entre Administraciones Públicas para ser empleados en el ejercicio de competencias o para materias distintas a las que motivaron su originaria recogida sin necesidad de recabar previamente el consentimiento del interesado (art. 11.1 LOPD, en relación con lo dispuesto en los arts. 4.1 y 2 y 5.4 y 5), es decir, la cesión de datos inconsentida autorizada por una norma infralegal, soslaya que el art. 53.1 CE reserva en exclusiva a la Ley la regulación y limitación del ejercicio de un derecho fundamental, vulnerando por consiguiente el derecho fundamental mismo, al privarle de una de sus más firmes garantías"* (Fundamento Jurídico 2).

En este sentido, el art. 53.1 de la Constitución Española señala que *"los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161.1.a)"*.

Por tanto, salvo en la cesión entre Administraciones Públicas para el ejercicio de competencias idénticas o que versen sobre las mismas materias, rige el principio de reserva de Ley, de tal modo que, a falta de consentimiento, expreso o tácito cuando la Ley lo permita, del afectado, será necesaria la existencia de una norma con rango de Ley habilitante de la cesión, sin perjuicio de que la misma quede o no posteriormente concretada en una norma reglamentaria dictada en su desarrollo.

Este criterio ha sido ratificado por el 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, señalando en su artículo 10.2.a) que será posible la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

- El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

- El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

4.5. ¿Puede un centro de enseñanza de carácter público ceder los datos del alumnado a una editorial especializada en literatura juvenil, que desee lanzar una nueva colección literaria especialmente orientada a los jóvenes, sin el consentimiento de aquéllos?

No. Conforme a lo establecido en el art. 11 LOPD, que regula las cesiones o comunicaciones de datos, *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"* (art. 11.1 LOPD). Asimismo, *"Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar"* (art. 11.3 LOPD).

Por tanto, será necesario contar con el consentimiento previo e informado para poder ceder los datos a la editorial, para lo cual es necesario que los alumnos y alumnas sean advertidos previamente de que sus datos serán facilitados a una editorial especializada en literatura juvenil para ofrecerles la nueva colección literaria que desea lanzar al mercado. En este mismo sentido, habrá que atender a la edad del alumnado para determinar si el consentimiento para la citada cesión debe ser otorgado por ellos mismos o por sus padres, madres o representantes legales, en función de sus condiciones de madurez.

4.6. Un centro de enseñanza desea organizar una visita guiada para los alumnos y alumnas menores de catorce años a un planetario, solicitándole éste un listado de todos aquellos que vayan a participar en dicha actividad. ¿Qué medidas debería tomar el centro de enseñanza con respecto al cumplimiento de principios de la LOPD?

El centro de enseñanza debería tener en cuenta lo establecido en los apartados 1 y 3 del art. 11 de la Ley Orgánica 15/1999, solicitando el consentimiento previo e informado de los padres, madres o representantes legales de los alumnos y alumnas para poder ceder sus datos al planetario.

Un cauce apropiado para informar sobre la finalidad de dicha cesión y solicitar el consentimiento correspondiente por parte del centro de enseñanza sería incorporando la pertinente cláusula legal en el mismo documento donde se solicite la autorización de los padres, madres o representantes legales de los alumnos y alumnas para realizar la visita al planetario.

4.7. ¿Es necesario el consentimiento expreso y por escrito de los alumnos y alumnas o de sus padres, madres o representantes legales para la cesión de determinados datos que consten en su expediente académico para realizar el cambio de un centro de enseñanza a otro?

No. El art. 11 LOPD, que regula las cesiones o comunicaciones de datos, establece expresamente que *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"* (art. 11.1 LOPD). Ahora bien, dicho consentimiento no será preciso, tal y como establece el art. 11.2.a), cuando la cesión está autorizada en una ley.

En este sentido, el apartado segundo de la Disposición adicional vigesimotercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOE) establece que *"La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos"*.

Por tanto, no será necesario el consentimiento expreso y por escrito de los alumnos y alumnas o de sus padres, madres o representantes legales para la cesión de determinados datos que consten en su expediente académico, siempre y cuando se haga con la exclusiva finalidad de realizar el cambio de un centro de enseñanza a otro.

4.8. ¿Puede ceder el centro de enseñanza los datos del alumnado a la Asociación de Madres y Padres de Alumnos (AMPA) sin su consentimiento previo?

No. El art. 11 LOPD, que regula las cesiones o comunicaciones de datos, establece expresamente que *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"* (art. 11.1 LOPD).

En este sentido, la Asociación de Madres y Padres de Alumnos (AMPA) es una entidad con personalidad jurídica propia e independiente del centro de enseñanza. De tal manera, será necesario que el centro solicite el consentimiento previo e informado para poder comunicar los datos a la AMPA. A este respecto, habrá que atender a la edad de los alumnos y alumnas para determinar si el consentimiento para la citada cesión debe ser otorgado por ellos mismos o por sus padres, madres o representantes legales, en función de sus condiciones de madurez.

4.9. Si los miembros de las Fuerzas y Cuerpos de Seguridad solicitan la cesión de los datos del alumnado, ¿debería el centro facilitar los citados datos?

El art. 22 de la Ley Orgánica 15/1999, de 13 de diciembre (en adelante, LOPD) establece una regulación específica para los ficheros de datos de carácter personal responsabilidad de las Fuerzas y Cuerpos de Seguridad.

De tal manera, existe una excepción al principio general del consentimiento en lo que respecta a la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad, si bien con determinados límites: *"la recogida y tratamiento automatizado para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real y grave para la seguridad pública o para la*

represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad" (art. 22.2 LOPD).

Asimismo, con respecto a las solicitudes de datos especialmente protegidos por parte de las Fuerzas y Cuerpos de Seguridad, el art. 22 LOPD establece en su apartado 3 que "*la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales"*.

Por tanto, el citado artículo de la Ley Orgánica 15/1999 habilita a los miembros de las Fuerzas y Cuerpos de Seguridad para la obtención y tratamiento de los datos del alumnado requeridos a los centros de enseñanza, lo que lleva aparejada la procedencia de la cesión, siempre y cuando se cumplan las siguientes condiciones:

- En primer lugar, ha de quedar debidamente acreditado que los datos solicitados al centro de enseñanza son necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales o que, tratándose de datos especialmente protegidos, son absolutamente necesarios para los fines de una investigación concreta.

- Asimismo, la solicitud de datos del alumnado por parte de las Fuerzas y Cuerpos de Seguridad ha de realizarse con la debida motivación, que acredite su relación con los supuestos anteriormente indicados.

- En tercer lugar, la solicitud ha de efectuarse con respecto a unos datos concretos y específicos de uno, una o varios o varias alumnos o alumnas, no teniendo encaje legal las solicitudes masivas de datos de todo el alumnado.

- Finalmente, los datos solicitados al centro de enseñanza habrán de ser cancelados de los ficheros específicos responsabilidad de las Fuerzas y Cuerpos de Seguridad cuando dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento, de conformidad a lo establecido en el apartado 4 del citado art. 22 LOPD. A estos efectos, deberán ser tenidos en consideración la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

4.10. Si un centro de enseñanza decide ambientar su página web con imágenes difuminadas o distorsionadas del alumnado, de manera que sean totalmente irreconocibles las personas que en ellas aparecen, ¿sería necesario contar con su consentimiento para la publicación de las citadas imágenes?

En principio, no. En este sentido, la Agencia Española de Protección de Datos archivó en diciembre de 2006 la denuncia presentada por un particular que alegaba la publicación, sin su consentimiento previo, de su fotografía en el apartado *"foro"* de una página web. La razón del archivo de la citada denuncia fue el tamaño mínimo -2,45 Kilobytes-, actitud y carácter de la toma fotográfica, que no permitían la identificación de la persona fotografiada. Profundizando sobre esta cuestión, la AEPD indicó lo siguiente:

"Con relación a esta cuestión, y en cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 señala que "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"; definiéndose el concepto de dato de carácter personal en el artículo 3.a) de la citada LOPD como "Cualquier información concerniente a personas físicas identificadas o identificables".

El artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la LOPD, considera datos de carácter personal "toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable" (el subrayado es de la Agencia Española de Protección de Datos).

En este mismo sentido, se pronuncia el artículo 2.a) de la Directiva 95/46/CE, del Parlamento y del Consejo, de 24/10, 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, según el cual se entiende por datos personales "toda información sobre una persona física identificada o identificable ("el interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social" (el subrayado es de la Agencia Española de Protección de Datos)." (Resolución de Archivo de Actuaciones de 20 de diciembre de 2006, Expediente Nº: E/00357/2005, Fundamento de Derecho III).

Por tanto, dado que la imagen publicada en la página web no permitía identificar ni hacer identificable a persona alguna, la AEPD entendió que no era aplicable la normativa sobre protección de datos de carácter personal al supuesto concreto, no siendo necesario, por tanto, el consentimiento previo del interesado para la publicación de la misma.

4.11. Un periódico local desea hacer un reportaje gráfico en el centro de enseñanza, en el cual se incluyan imágenes del alumnado en diferentes momentos de la actividad escolar. ¿Qué precauciones debería tomar el centro con respecto a la normativa sobre protección de datos de carácter personal?

Conforme a lo establecido en el artículo 2.a) de la 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, se entiende por dato personal *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*.

Atendiendo a la citada definición, que considera dato de carácter personal *"toda información sobre una persona física identificada o identificable"*, las fotografías publicadas en el reportaje gráfico realizado por el periódico local se ajustarán a este concepto siempre que permitan la identificación de las personas que aparecen en dichas imágenes.

El 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, también considera la imagen como un dato de carácter personal, al definir como tal *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"* (art. 5.1.f)).

Por tanto, la consideración de las fotografías que permitan la identificación de las personas objeto de las mismas (esto es, el alumnado) como datos de carácter personal, lleva aparejada la indisoluble aplicación de los principios de protección de datos establecidos en la Directiva 95/46/CE y en la Ley Orgánica 15/1999, que es transposición de la misma.

En este sentido, el apartado 1 del artículo 6 de la LOPD establece expresamente que *"el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa"*. Por tanto, será necesario solicitar el consentimiento del alumnado o de sus padres, madres o representantes legales, en función de sus condiciones de madurez, con carácter previo a la publicación de sus imágenes en el reportaje gráfico del periódico local sobre el centro de enseñanza.

4.12. Ante el inminente comienzo de las revisiones médicas y campañas de vacunación del alumnado de los centros de enseñanza, la Consejería de Sanidad solicita a éstos un listado de los mismos para poder llevarlas a cabo. ¿Qué requisitos deberían observar los centros de enseñanza para que dicha cesión de datos fuese conforme a la normativa sobre protección de datos de carácter personal?

El art. 11 LOPD, que lleva por rúbrica *"Comunicación de datos"*, establece, como regla general, que *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"*. Por tanto, en principio, será requisito imprescindible el consentimiento previo del alumnado o de sus padres, madres o representantes legales, según proceda, para poder llevar a cabo la citada cesión de datos de carácter personal a la Consejería de Sanidad.

Ahora bien, el art. 11.2.a) establece una excepción al principio general del consentimiento *"cuando la cesión está autorizada en una ley"*. De tal manera, si la citada cesión de datos de carácter personal a la Consejería de Sanidad, para la realización de las correspondientes revisiones médicas y campañas de vacunación del alumnado, está autorizada en alguna norma con rango de Ley, no será necesario el consentimiento previo del alumnado o de sus padres, madres o representantes legales.

5. Datos especialmente protegidos

5.1. ¿Tiene el dato de opción por la asignatura de Religión la consideración de dato especialmente protegido?

No. Dicha cuestión fue formulada a la Agencia Española de Protección de Datos en el año 2002, interpretando ésta lo siguiente:

"Como punto de partida, el artículo 7.2 de la Ley Orgánica 15/1999 dispone que "sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias", prohibiendo el artículo 7.4 "los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual". Estas previsiones deben ponerse en conexión con lo establecido en el artículo 7.1 de la Ley Orgánica, a cuyo tenor "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias". Dicho precepto es una mera reproducción de lo establecido, a su vez, en el artículo 16.2 de la Constitución.

De este modo, ha de considerarse que los datos a los que se refiere el artículo 7.2 de la Ley Orgánica 15/1999 son aquéllos que efectivamente se encuentran directamente vinculados con las creencias religiosas, filosóficas, políticas o morales de la persona, protegidas constitucionalmente a través del derecho fundamental a la libertad ideológica, religiosa y de culto, consagrado por el artículo 16.1 de la Constitución.

Sentados así los términos de interpretación de lo establecido en el artículo 7.2 de la Ley Orgánica 15/1999, debe ahora plantearse si el hecho de cursar la asignatura de religión, o el hecho de no cursarla, suponen la revelación de un dato protegido por el citado derecho fundamental, que coadyuva a la especial protección que también confiere la LOPD, es decir, si ese dato revela efectivamente las convicciones religiosas de la persona a la que se refiere.

Pues bien, el hecho mismo de cursar la asignatura de religión no revela necesariamente que el estudiante profese las creencias a las que tal asignatura se refiere, del mismo modo que el hecho de no cursarla no revela la inexistencia de esas creencias, sino que tal circunstancia puede deberse al estudio de la religión en otros foros distintos del escolar. Es decir, a nuestro juicio, lo único que revela el dato de optar por cursar la asignatura de religión sería el interés del alumno por conocer los principios, historia y preceptos de la misma, sin que ello implique una efectiva confesionalidad del mismo, a cuya declaración no podría encontrarse obligado.

Por este motivo, el dato relacionado con el hecho de que el alumno curse la asignatura de religión, no vinculada a la participación del alumno en un rito relacionado con una religión determinada (lo que sí implicaría que el individuo profesa dicha creencia religiosa) y no puede ser considerado por sí mismo un dato que revele inmediatamente las creencias religiosas del afectado, por lo que su régimen no se encuentra sometido a lo establecido en las normas que se citaron anteriormente, dado que el dato no tendría la naturaleza de especialmente protegido."

5.2. ¿Qué consideración tienen los datos psicológicos incluidos en los informes elaborados por los orientadores y orientadoras?

Los orientadores y orientadoras de los centros suelen confeccionar informes psicopedagógicos, test de inteligencia y conducta, etc. Para su elaboración, es necesario recabar una serie de información concerniente a cada uno de los alumnos del centro, incluyendo datos psicológicos.

Sobre la función orientadora en los centros de enseñanza de la Junta de Andalucía, cabe citar las siguientes normas autonómicas:

- El Decreto 213/1995, de 12 de septiembre, por el que se regulan los Equipos de Orientación Educativa.
- La Orden de 23 de julio de 2003, por la que se regulan determinados aspectos sobre la organización y el funcionamiento de los Equipos de Orientación Educativa.
- El Reglamento Orgánico de los Institutos de Educación Secundaria,

aprobado por Decreto 200/1997, de 3 de septiembre, que establece la composición y funciones de los Departamentos de Orientación, así como las funciones de los orientadores u orientadoras.

- La Orden de 27 de julio de 2006, por la que se regulan determinados aspectos referidos a la organización y funcionamiento del departamento de orientación en los Institutos de Educación Secundaria.

Sobre los Equipos de Orientación Educativa, el Decreto 213/1995 los define como *"unidades básicas de orientación psicopedagógica que, mediante el desempeño de funciones especializadas en las áreas de orientación educativa, atención a los alumnos y alumnas con necesidades educativas especiales, compensación educativa y apoyo a la función tutorial del profesorado, actúan en el conjunto de los centros de una zona"* (art. 1).

En lo que respecta a los Departamentos de Orientación, el Reglamento Orgánico de los Institutos de Educación Secundaria asigna a los mismos la función de elaborar la propuesta del Plan de Orientación y Acción Tutorial, así como un conjunto de funciones relacionadas con la orientación académica, psicopedagógica y profesional, con la evaluación psicopedagógica de los alumnos y alumnas que la requieran y con el apoyo a la acción tutorial, todo ello en el marco de la atención a las diversas aptitudes, intereses y motivación del alumnado.

Con respecto a la naturaleza de los datos psicológicos, en 1999 se planteó a la AEPD por parte de una Corporación Local la posibilidad de proceder, dentro del tratamiento de los datos efectuado en el ámbito de sus competencias en materia de asistencia social, al tratamiento de datos de carácter psicológico, incluyendo determinados datos, obtenidos de la apreciación subjetiva de las personas encargadas de llevar a cabo la realización material de encuestas, referentes a los "problemas" que presenta el perfil psicológico de los sujetos encuestados (tales como dificultades en el aprendizaje, alcoholismo, drogodependencia, ludopatía, conflictos de pareja, síntomas depresivos, conflictos de adaptación al medio familiar o social, desarraigo, etc.).

Sobre la naturaleza de los datos psicológicos, la cuestión radica en delimitar si procede su inclusión dentro del concepto de datos referentes a la salud de las personas. Si bien la Ley Orgánica se refiere expresamente a los datos de salud, considerándolos expresamente protegidos y limitando la posibilidad de su recopilación y cesión, no establece un concepto concreto de este tipo de datos. La AEPD ha entendido que los datos psicológicos obtenidos deben ser considerados, a los efectos de la aplicación de la LOPD, como datos relativos a la salud de las personas, habida cuenta que, o bien conciernen directamente a la salud mental del individuo o bien se encuentran estrechamente relacionados con la salud.

De hecho, el Informe 0572/2009, del Gabinete Jurídico de la Agencia Española de Protección de Datos, referente a las medidas de seguridad aplicables a los ficheros con datos académicos, dice textualmente: *"No obstante, debe indicarse que si el fichero contuviera datos referentes al perfil psicológico de los afectados y que hicieran referencia a la existencia de anomalías o especialidades de la personalidad del sujeto, habrá de considerarse que el fichero contiene datos relacionados con la salud de las personas, siendo entonces de aplicación lo dispuesto en el artículo 81.3.a) del Reglamento 1720/2007, que exige la adopción sobre estos ficheros de las medidas de seguridad de nivel alto, además de las medidas de nivel básico y medio".*

Por tanto, de acuerdo a la interpretación de la AEPD, el nivel de protección que correspondería aplicar a los informes elaborados por los orientadores y orientadoras sería Nivel alto.

5.3. ¿Tiene el dato de origen racial del alumnado del centro de enseñanza la consideración de dato especialmente protegido?

Sí. El art. 7 de la Ley Orgánica 15/1999, configura bajo la rúbrica general de *"Datos especialmente protegidos"*, un régimen especialmente cualificado, con protección mas intensa, para aquellos datos personales que proporcionan una información de esferas íntimas del individuo (Sentencia de la Audiencia Nacional de fecha 12 de abril de 2002, recurso 1271/2000). En este sentido, el art. 7.3 LOPD establece que *"Los datos*

de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".

Por tanto, en caso de que un centro de enseñanza necesite recabar, tratar o ceder a terceros organismos o entidades datos referentes al origen racial del alumnado, es requisito previo imprescindible que una norma con rango de Ley así lo disponga o bien se haya consentido expresamente por parte del alumno, la alumna o su padre, madre o representante legal, cuando así proceda, para su recogida y posterior tratamiento.

Asimismo, es importante recordar que, cuando se recojan datos de esta naturaleza, debe respetarse escrupulosamente el principio de calidad de los datos establecido en el art. 4 LOPD. De tal manera, los datos recogidos han de ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente. Así por ejemplo, podría tener la consideración de excesivo el dato de origen racial recabado para realizar un estudio sobre salud respiratoria y nivel de alergias en los centros de enseñanza, ya que, en principio, el origen racial no es un dato necesario para determinar si una persona padece o no alergia.

5.4. ¿Qué naturaleza tienen los ficheros manejados por el profesorado sobre calificaciones parciales, conductas y actitudes del alumnado, entrevistas con los padres y madres, etc.?

En principio, los citados ficheros están constituidos por datos catalogados como de nivel básico, salvo que contengan datos especialmente protegidos, tales como datos referentes a la salud del alumnado, incluyendo posibles datos psicológicos (ya que conciernen directamente a la salud mental del alumnado), o sobre su origen racial, en cuyo caso deberían encajarse dentro del nivel alto definido en el Título VIII del Real Decreto 1720/2007.

No obstante, si el fichero en cuestión contiene un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los alumnos y alumnas del centro y que permitan evaluar

determinados aspectos de la personalidad o del comportamiento de los mismos, estaríamos en el nivel medio contemplado en el Título VIII del Real Decreto 1720/2007.

La Real Academia Española de la Lengua define la *"personalidad"*, entre otras acepciones, como el *"conjunto de cualidades que constituyen a la persona o sujeto inteligente"*. De tal manera, parece que un fichero en el cual se contuviesen datos sobre conductas y actitudes del alumnado, así como información sobre el mismo obtenida a través de entrevistas con los padres y madres, sí permitiría obtener una evaluación de determinados aspectos de la personalidad o del comportamiento de los alumnos y alumnas del centro.

Que las medidas de seguridad a adoptar sean las de nivel medio, se desprende del reciente Informe del Gabinete Jurídico de la Agencia Española de Protección de Datos (Informe 0572/2009) que establece: *"Esta Agencia ha venido señalando respecto a la interpretación que daba darse al artículo 81.2.f) que de dicho precepto se desprende que su finalidad es someter a criterios de seguridad más rigurosos aquellos ficheros que permitan obtener una información adicional sobre el afectado, obteniendo así un perfil de situación económica o familiar o de sus aficiones, preferencias, etc. Así, se encontrarán comprendidos en dicho artículo todos los ficheros que contengan datos a partir de los cuales puedan deducirse cualquiera de las facetas antes mencionadas o, como sucede en el presente caso, se incluyan datos relativos al rendimiento académico que permitan deducir un perfil de estudios."*

En su consecuencia, salvo mejor criterio, parece que el nivel más lógico a asignar a los citados ficheros sería el nivel medio contemplado en el Título VIII del Real Decreto 1720/2007.

6. Principio de información

6.1. En el supuesto de que una empresa de chocolatinas deseara organizar, en colaboración con el centro de enseñanza, un concurso de dibujo para cuya participación los alumnos y alumnas debieran facilitar sus datos y rellenar un cuestionario sobre sus gustos alimenticios, ¿qué factores debería tener en cuenta el centro?

Debería tenerse en cuenta lo establecido en los arts. 5 y 6 de la Ley Orgánica 15/1999, esto es, el deber de información y el principio del consentimiento con respecto a la recogida y posterior tratamiento de los datos del alumnado del centro por parte de la empresa de chocolatinas. De igual manera, habría que tener en cuenta lo dispuesto en el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, dedicado al consentimiento para el tratamiento de datos de menores de edad, donde entre otros aspectos se diferencia entre los mayores y menores de 14 años resultando, en este último caso, de obligado cumplimiento la prestación del consentimiento por parte de padres o tutores para el tratamiento de sus datos.

De tal manera, la citada empresa debería informar escrupulosamente al alumno, la alumna o su padre, madre o representante legal, cuando así proceda, con carácter previo a la recogida de sus datos, de la finalidad para la que éstos se recogen, de los destinatarios de la información que faciliten, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos y de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, así como de la identidad y dirección del responsable del tratamiento. Asimismo, debería solicitar el consentimiento de las personas citadas para el tratamiento y cesión de los datos solicitados.

En caso de que la empresa no siguiese las pautas indicadas, el centro no debería colaborar con ella para la organización del concurso de dibujo. Tal como señala GISBERT JORDÁ, el sector infantil y juvenil constituye un punto de creciente atención en los últimos años por parte del marketing comercial que lo considera un mercado de gran potencial en expansión.

Ello se traduce en la necesidad de un comportamiento ético, honesto, transparente y respetuoso con la legislación vigente por parte de las empresas con respecto al tratamiento de los datos de carácter personal de clientes y consumidores, que adquiere además una especial dimensión y trascendencia cuando se trata de datos de niños, niñas y adolescentes.

7. Principio de calidad de los datos

7.1. Un centro de enseñanza de carácter público solicita, para la admisión de los alumnos y alumnas, el dato sobre la confesión religiosa de sus padres y madres. ¿Sería ello correcto conforme a lo establecido en los principios de la LOPD?

No, ya que tendría la consideración de dato excesivo. En este sentido, el art. 4 LOPD, que regula el principio de calidad de los datos, establece expresamente que *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"* (art. 4.1 LOPD).

Por tanto, dado que la confesión religiosa de los padres y madres no es un dato necesario para tramitar la solicitud de plaza ni la matriculación del futuro alumno o alumna en el centro de enseñanza, ni tampoco para el mantenimiento de su futura relación con el mismo, tendría, como hemos indicado, la consideración de dato excesivo.

8. Acceso a los datos por cuenta de terceros

8.1. Un centro de enseñanza tiene contratado el servicio de transporte escolar con una empresa de autobuses, la cual además de hacer el transporte diario de los alumnos y alumnas, recoge un listado de los mismos y de las mismas para hacer los carnés de acceso a dicho servicio de transporte. ¿Qué medidas debería tomar el centro para adecuar tal comunicación de datos a la LOPD?

En este caso, la empresa de autobuses tendría la consideración de *"encargado de tratamiento"*, puesto que para prestar un servicio al centro de enseñanza necesita tratar los datos de los alumnos y alumnas del mismo.

Según establece el artículo 12 de la LOPD, la relación entre el responsable del fichero y el encargado del tratamiento debe regularse por medio de un contrato celebrado por escrito. En dicho contrato debe especificarse que los datos serán tratados por el encargado del tratamiento según las indicaciones recibidas por el responsable del fichero y exclusivamente para la finalidad pactada entre ambas partes. También deben establecerse las medidas de seguridad que deberá cumplir el encargado del tratamiento para efectuar dicho tratamiento de datos personales. Una vez finalizada la prestación del servicio, los datos personales a los que haya tenido acceso el encargado del tratamiento deberán ser devueltos al responsable del fichero, así como cualquier otro tipo de soporte o documento en los que consten los mismos.

No se debería obviar lo establecido en el artículo 22.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, que completa al mencionado artículo 12 de la LOPD, estableciendo la obligación del encargado del tratamiento de conservar debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

8.2. Un centro de enseñanza tiene en sus dependencias unos contenedores destinados al reciclaje de papel. Cada cierto tiempo dichos contenedores son retirados por una empresa de reciclaje. ¿Qué medidas debería llevar a cabo el centro para cumplir con los principios de LOPD?

En primer lugar, el centro de enseñanza debería tener firmado con la empresa de reciclaje el contrato que se regula en el artículo 12 de la LOPD, puesto que dicha empresa tendría la consideración de *"encargado de tratamiento"*, ya que en el desempeño de la prestación de servicios de reciclaje de papel tiene o podría tener acceso a documentos con datos de carácter personal (por ejemplo, datos del alumnado del centro).

Además de lo anterior, sería interesante que el centro contase con destructoras de papel y las utilizase con los documentos que pudieran contener datos de carácter personal antes de que los mismos fuesen depositados en los contenedores destinados al reciclaje de papel.

9. Deber de secreto

9.1. ¿En qué consiste el deber de secreto?

La Ley Orgánica 15/1999 establece en su art. 10 un deber de secreto para todo aquél que tenga acceso a los datos de carácter personal gestionados en el centro en el desempeño de sus funciones. En este sentido, no es necesario que exista una dependencia laboral, funcionarial o administrativa indefinida para que la persona con acceso al fichero esté sometida al deber de secreto, el desempeño de cualquier prestación o trabajo que permita el acceso a datos de carácter personal (por ejemplo, datos del alumnado del centro) genera automáticamente la obligación de cumplir con este principio.

De igual manera, no debe confundirse este deber de secreto con el secreto profesional al que están sometidas determinadas personas en función de la profesión que ejercen. Este deber de secreto es un deber genérico que alcanza a cualquier persona que intervenga en el tratamiento de los datos, ya sea personal docente, psicólogos/as, pedagogos/as, logopedas y orientadores/as escolares, personal administrativo, conserjes, personal de limpieza o cualquier otro.

9.2. ¿Puede el Presidente de la Comisión de Baremación de las solicitudes de reserva para la matriculación en una escuela infantil municipal hacer públicos los datos procedentes de los certificados del IRPF presentados por el padre y la madre de una alumna admitida en la misma?

No. Tal y como señaló la Agencia Española de Protección de Datos en su Resolución R/00597/2006, de 8 de septiembre de 2006, el que el Presidente de la Comisión de Baremación de las solicitudes de reserva para la matriculación en una escuela infantil municipal haga públicos los datos del padre y la madre de una alumna admitida en la misma, relativos a la renta familiar líquida mensual de la unidad familiar, supone una vulneración del deber de guardar secreto contemplado en el art. 10 LOPD, ya que dichos datos son obtenidos a través de los certificados del IRPF, presentados con la exclusiva finalidad de solicitar la admisión y reserva de plaza de su hija, lo cual no autoriza al Presidente de la Comisión de Baremación para hacer públicos dichos datos en otros foros.

10. Medidas de Seguridad

10.1. ¿Puede el profesorado crear nuevos ficheros ofimáticos que contengan datos de carácter personal, en los PC's del centro de enseñanza, sin el conocimiento de la Secretaría General Técnica de la Consejería de Educación?

No. En principio, la Secretaría General Técnica de la Consejería de Educación es la responsable de los ficheros de datos de carácter personal tratados en los centros públicos de la Junta de Andalucía. En este sentido, el profesorado de los centros de enseñanza, como mero usuario de los mismos, no está autorizado para crear nuevos ficheros que contengan datos de carácter personal.

En este sentido, la LOPD califica como infracción grave *"Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente"* (art. 44.3.a) LOPD).

Asimismo, la Ley Orgánica 15/1999 establece que *"no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y*

a las de los centros de tratamiento, locales, equipos, sistemas y programas" (art. 9.2 LOPD).

De tal manera, en el supuesto de la creación de nuevos ficheros ofimáticos con datos de carácter personal que no incorporasen las medidas exigidas en el Título VIII del Real Decreto 1720/2007 en cuanto a identificación y autenticación, copias de respaldo y recuperación, etc., se estaría incurriendo en una infracción grave, contemplada en el art. 44.3.d) LOPD: *"Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave"*.

10.2. En el supuesto de que el personal docente del centro se lleve los exámenes realizados por el alumnado para corregirlos en casa, ¿qué precauciones habría que tener en cuenta con respecto a la normativa de protección de datos de carácter personal?

En primer lugar, debemos señalar que los exámenes contienen, en principio, datos de carácter personal del alumnado catalogados como de nivel básico (nombre y apellidos, curso, DNI, firma, calificación, etc.).

A efectos de lo preceptuado en el 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, los exámenes tendrían la consideración de *"documento"*, entendiendo por tal *"todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada"* (art. 5.2.f) del Real Decreto 1720/2007).

En este sentido, serán de aplicación las medidas de seguridad de nivel básico contempladas en el Título VIII del Real Decreto 1720/2007 en referencia a la gestión de documentos, así como lo señalado en referencia al régimen de trabajo fuera de los locales del responsable del fichero.

En primer lugar, el artículo 92 del Real Decreto 1720/2007, relativo a la gestión de documentos, establece las siguientes obligaciones en referencia a la salida de los exámenes del centro para su corrección por el personal docente:

- La salida de los exámenes fuera de los locales del centro deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

- En el traslado de los exámenes se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

- Siempre que vaya a desecharse cualquier examen deberá procederse a su destrucción, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Por otro lado, el artículo 86 del Real Decreto 1720/2007, referente al régimen de trabajo fuera de los locales del responsable del fichero, establece las siguientes obligaciones:

- Cuando los datos de carácter personal se traten fuera de los locales del responsable de fichero o tratamiento (por ejemplo, la corrección de los exámenes que contienen datos del alumnado fuera del centro, en casa del docente), será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

- La citada autorización deberá constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

De igual manera, el personal docente que se lleve los exámenes a casa queda sujeto al correspondiente *"deber de secreto"*, establecido en el art. 10 LOPD.

10.3. ¿Qué ocurriría si se dejasen abandonados en plena calle, junto a un contenedor de reciclaje de papel saturado, informes psicopedagógicos sobre antiguos alumnos y alumnas elaborados por los orientadores y orientadoras, de manera que alguien externo al centro de enseñanza tuviese acceso a dicha información?

A efectos de lo preceptuado en el 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, los informes psicopedagógicos sobre antiguos alumnos y alumnas elaborados por los orientadores y orientadoras tendrían la consideración de *"documento"*, entendiendo por tal *"todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada"* (art. 5.2.f) del Real Decreto 1720/2007).

En este sentido, el artículo 92 del Real decreto 1720/2007, referente a la gestión de documentos, establece en su apartado cuatro que *"siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior"*.

De tal manera, en el caso de que se encontrasen abandonados en la vía pública una serie de informes psicopedagógicos en papel, se estaría incurriendo en una infracción grave prevista en el artículo 44.3.h) de la LOPD: *"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que*

por vía reglamentaria se determinen". Ello es así porque no se han adoptado las medidas necesarias para impedir cualquier acceso o recuperación posterior de la información contenida en los informes psicopedagógicos conforme a lo establecido en el artículo 92 del Real decreto 1720/2007, por ejemplo habiendo procedido previamente al triturado de los mismos.

En segundo lugar, podríamos estar ante un incumplimiento del deber de secreto establecido en el artículo 10 de la LOPD, el cual estipula que *"el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*. El incumplimiento del citado deber de secreto, en principio, constituye una infracción tipificada como leve en el artículo 44.2.e) de la LOPD. En el caso de que se trate de la vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito o aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo, estaríamos ante una infracción grave de acuerdo a lo tipificado en el artículo 44.3.g) de la LOPD. Finalmente, en el caso de que la vulneración del deber de guardar secreto sea acerca de datos especialmente protegidos (tal como sucede en este caso, en virtud de lo establecido en el Informe 0572/2009 de la Agencia Española de Protección de Datos) estaremos ante una infracción muy grave conforme a lo tipificado en el artículo 44.4.g) de la LOPD.

En resumen, en el caso de unos informes psicopedagógicos abandonados junto a un contenedor en plena vía pública estaríamos ante una posible vulneración del principio de seguridad de los datos, así como ante un posible incumplimiento del deber de secreto.

10.4. ¿Es correcto dejar en los pasillos del centro y, por tanto, al alcance de cualquier persona que por allí transite, los contenedores de reciclaje que puedan contener exámenes realizados por el alumnado, sin haber sido destruidos previamente?

No. Los datos de carácter personal contenidos en los exámenes realizados por el alumnado deben estar protegidos hasta el momento de su destrucción física o reciclado. De tal manera, los contenedores donde se almacenen los mismos no deben permanecer al descubierto en el exterior de los edificios, ni en lugares de paso (por ejemplo, en los pasillos del centro).

En caso contrario, podríamos estar ante un incumplimiento del deber de secreto establecido en el artículo 10 de la LOPD, el cual estipula que *"el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*. El incumplimiento del citado deber de secreto, en principio, constituye una infracción tipificada como leve en el artículo 44.2.e) de la LOPD.

Una alternativa valorable es destruir los exámenes con carácter previo a su depósito en el contenedor de reciclaje (por ejemplo, mediante destructoras de papel), de manera que sea imposible la recuperación de la información contenida originariamente en los mismos por parte de terceros.

10.5. ¿Qué precauciones deben tomarse con respecto a la normativa de protección de datos de carácter personal en el caso de traslado de documentación que contenga datos catalogados de nivel alto (por ejemplo, informes psicopedagógicos)?

El artículo 114 del 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, relativo al traslado de documentos que contengan datos de carácter personal de nivel alto, establece que *"siempre que se proceda al traslado físico de la*

documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado".

Por tanto, en el supuesto del envío o traslado de documentación que contenga datos de carácter personal catalogados de nivel alto, se recomienda la adopción de medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

10.6. ¿Quién es el responsable de informar al profesorado y Personal de Administración y Servicios sobre sus obligaciones en materia de protección de datos de carácter personal?

Conforme a lo establecido en el art. 89.2 del 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, *"El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento"*.

En principio, la Secretaría General Técnica de la Consejería de Educación es la responsable de los ficheros de datos de carácter personal tratados en los centros públicos de la Junta de Andalucía, ya que éstos no poseen personalidad jurídica independiente de la misma. Por tanto, será ésta quien, bien directamente o bien delegando expresamente en cada uno de los centros, está obligada a informar al profesorado y Personal de Administración y Servicios sobre sus obligaciones en materia de protección de datos de carácter personal.

10.7. ¿Qué ocurriría en el supuesto de que un o una docente tuviese acceso a un documento impreso con información sobre el personal del centro de enseñanza restringida al equipo directivo y personal de Administración?

El artículo 91 del 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, relativo al *"Control de acceso"*, establece lo siguiente:

- Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

- El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

- El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

- Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

- En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Un documento impreso con información sobre el personal del centro de enseñanza podría tener la consideración de *"recurso"* a efectos de lo establecido en el Real Decreto 1720/2007, que entiende por tal *"cualquier parte componente de un sistema de información"* (art. 5.2.k)). En este sentido, le serían de aplicación las medidas de seguridad contempladas en el artículo 91 del citado Real Decreto.

Asimismo, el apartado primero del artículo 113 del Real Decreto 1720/2007, relativo al *"Acceso a la documentación"*, establece que *"el acceso a la documentación se limitará exclusivamente al personal autorizado"*.

De tal manera, en el supuesto de que un o una docente tuviese acceso a un documento impreso con información sobre el personal del centro de enseñanza restringida al equipo directivo (Director o Directora, Secretario o Secretaria y Jefe o Jefa de Estudios) y personal de Administración, se estaría incurriendo en una infracción grave contemplada en el art. 44.3.h) LOPD: *"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen."*

Por todo ello, se recomienda que se configuren los protectores de pantalla de los puestos de trabajo de manera que se activen de manera automática cuando los usuarios deban abandonar temporalmente los mismos, siendo necesario introducir una contraseña para la reanudación del trabajo. De tal manera, se impide la visualización de los datos de la pantalla por parte de terceros no autorizados, así como las impresiones de los mismos.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

En el caso de las impresoras, se recomienda que los usuarios retiren los documentos de la bandeja de salida conforme los vayan imprimiendo, de manera que no queden al alcance de terceros no autorizados impresiones que contengan datos de carácter personal.

Mientras la documentación no se encuentre en los archivos existentes por estar siendo tramitada o revisada, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que sea accedida por persona no autorizada.

ANEXO I

MODELOS ORIENTATIVOS DE CLÁUSULAS LEGALES A INCORPORAR EN LOS IMPRESOS Y FORMULARIOS DE USO FRECUENTE EN LOS CENTROS DE ENSEÑANZA PARA LA RECOGIDA DE DATOS DE CARÁCTER PERSONAL

Es importante señalar que, conforme a lo interpretado por la Agencia Española de Protección de Datos en su Memoria 2000, en el caso del tratamiento y/o cesión de datos de personas menores de catorce años, será necesario informar a sus padres, madres o representantes legales. A partir de la citada edad, en principio, ya podrían decidir sobre el tratamiento y/o cesión de sus datos de carácter personal.

El reciente 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, ha ratificado el criterio interpretativo de la Agencia Española de Protección de Datos. De tal manera, el apartado 1 del artículo 13 del Real Decreto 1720/2007 sitúa definitivamente la barrera del consentimiento para el tratamiento de los datos de las personas menores de edad en los catorce años, señalando que *"podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela"* y que *"en el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores"*.

En este sentido, es importante recordar que el menor o la menor que padezca una enfermedad o deficiencia persistente de carácter físico o psíquico que le impida gobernarse por sí mismo o por sí misma podrá ser declarado o declarada incapaz por sentencia judicial, tal y como establecen los artículos 199 a 201 del Código Civil español, en cuyo caso necesitaría el complemento de la capacidad de los titulares de la patria potestad o tutela para poder consentir sobre el tratamiento de sus datos de carácter personal, con total independencia de si ha cumplido o no los catorce años de edad.

Asimismo, el artículo 13 del citado Real Decreto 1720/2007 establece que *"cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo"* (apartado 3).

De tal manera, la redacción del texto para cumplir con el deber de información conforme a lo establecido en nuestra normativa sobre protección de datos de carácter personal no debería ser la misma en el caso de que dicha información vaya dirigida a un menor que cuando esté orientada hacia una persona adulta. Por tanto, se antoja indispensable que cuando se informe al menor de los extremos contemplados en el artículo 5 de la Ley Orgánica 15/1999 se haga en un lenguaje sencillo y fácilmente comprensible, carente de conceptos jurídicos abstrusos. De lo contrario, el menor carecería de poder de disposición y control alguno sobre sus propios datos de carácter personal, escaparían a su control porque simplemente no se le está explicando qué utilización se va a hacer de sus datos de manera que él lo entienda.

Finalmente, debemos recordar que, en varios de los impresos y formularios de uso frecuente en los centros de enseñanza también se recogen datos de carácter personal de los padres, madres o representantes legales del alumnado, debiendo igualmente ser informados de los extremos contemplados en el art. 5 LOPD.

Siguiendo estos criterios, se han elaborado modelos orientativos de cláusulas legales para cada uno de los impresos y formularios de uso frecuente en los centros de enseñanza.

1. Modelos de cláusulas legales a incorporar en los Formularios de Solicitud de Plaza

1.1. Alumnado menor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Los datos de carácter personal de su hijo, hija o menor cuya representación legal ostenta, recogidos a través del Formulario de Solicitud de Plaza y cualesquier otros documentos que pudieran serle solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar la solicitud de admisión de su hijo, hija o menor cuya representación legal ostenta, en el centro de enseñanza. Asimismo, los destinatarios de sus datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley, de conformidad con lo establecido en el artículo 11.2.a) LOPD.
b) Todos los datos solicitados a través del Formulario de Solicitud de Plaza son de cumplimentación obligatoria.
c) De igual manera, usted consiente expresamente para el tratamiento y/o cesión de todos aquellos datos de salud de su hijo, hija o menor cuya representación legal ostenta necesarios para tramitar su solicitud de admisión en el centro de enseñanza, conforme a lo establecido en la legislación vigente.
d) Su negativa a suministrar los datos solicitados implica la imposibilidad de tramitar la solicitud de admisión de su hijo, hija o menor cuya representación legal ostenta, en el centro de enseñanza, pues son necesarios conforme a lo establecido en la legislación vigente.
e) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
f) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre, madre o representante legal.

1.2. Alumnado mayor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu solicitud de admisión en el centro de enseñanza.

Asimismo, te informamos de que, para poder tramitar tu solicitud de admisión en el centro de enseñanza, también necesitaremos dar a conocer tus datos a otras personas y entidades, entre las cuales estarían [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión].

Necesitaremos que nos facilites todos los datos que te pidamos, incluidos aquellos datos de salud que sean imprescindibles para poder tramitar tu solicitud de admisión en el centro de enseñanza. Si no nos facilitas todos los datos que te pidamos no podremos tramitar tu solicitud, ya que todos ellos son necesarios para tu admisión en el centro de enseñanza.

Finalmente, te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del alumno o alumna.

1.3. Padres, madres y representantes legales

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Sus datos de carácter personal, recogidos a través del Formulario de Solicitud de Plaza y cualesquier otros documentos que pudieran serle solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar la solicitud de admisión de su hijo, hija o menor cuya representación legal ostenta, en el centro de enseñanza. Asimismo, los destinatarios de sus datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley, de conformidad con lo establecido en el artículo 11.2.a) LOPD.

b) Todos los datos solicitados a través del Formulario de Solicitud de Plaza son de cumplimentación obligatoria.

c) De igual manera, usted consiente expresamente para el tratamiento y/o cesión de todos aquellos datos referentes a su salud necesarios para tramitar la solicitud de admisión de su hijo, hija o menor cuya representación legal ostenta en el centro de enseñanza, conforme a lo establecido en la legislación vigente.

d) Su negativa a suministrar los datos solicitados implica la imposibilidad de tramitar la solicitud de admisión de su hijo, hija o menor cuya representación legal ostenta, en el centro de enseñanza, pues son necesarios conforme a lo establecido en la legislación vigente.

e) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

f) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre y de la madre o del representante legal.

1.4. Modelo simplificado alumnado menor de 14 años y familiares o representantes

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, les informamos que los datos de carácter personal recogidos a través del Formulario de Solicitud de Plaza y cualesquier otros documentos que pudieran serles solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía , con la finalidad de tramitar la solicitud de admisión en el centro de enseñanza. Los destinatarios de los datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley. De igual manera, consienten expresamente para el tratamiento y/o cesión de todos aquellos datos de salud necesarios para tramitar la solicitud de admisión. Pueden ejercer los derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

1.5. Modelo simplificado alumnado mayor de 14 años

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu solicitud de admisión en el centro de enseñanza. Asimismo, te informamos de que también necesitaremos dar a conocer tus datos a otras personas y entidades, entre las cuales estarían [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión]. Te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

2. Modelos de cláusulas legales a incorporar en los Formularios de Matriculación

2.1. Alumnado menor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Los datos de carácter personal de su hijo, hija o menor cuya representación legal ostenta, recogidos a través del Formulario de Matriculación y cualesquier otros documentos que pudieran serle solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar la matrícula de su hijo, hija o menor cuya representación legal ostenta, en el centro de enseñanza, así como el ejercicio de la función docente y orientadora. Asimismo, los destinatarios de sus datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley, de conformidad con lo establecido en el artículo 11.2.a) LOPD.

b) Todos los datos solicitados a través del Formulario de Solicitud de Matriculación son de cumplimentación obligatoria.

c) De igual manera, usted consiente expresamente para el tratamiento y/o cesión de todos aquellos datos de salud de su hijo, hija o menor cuya representación legal ostenta, necesarios para tramitar su matrícula en el centro de enseñanza, así como el ejercicio de la función docente y orientadora, conforme a lo establecido en la legislación vigente.

d) Su negativa a suministrar los datos solicitados implica la imposibilidad de formalizar la matriculación de su hijo, hija o menor cuya representación legal ostenta en el centro de enseñanza, pues son necesarios para la gestión y mantenimiento de la relación del centro con sus alumnos y alumnas.

e) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

f) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre, madre o representante legal.

2.2. Alumnado mayor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu matrícula en el centro de enseñanza, así como el ejercicio de la función docente y orientadora.

Asimismo, te informamos de que, para poder tramitar tu matrícula en el centro de enseñanza, así como el ejercicio de la función docente y orientadora, también necesitaremos dar a conocer tus datos a otras personas y entidades, entre las cuales estarían [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión].

Necesitaremos que nos facilites todos los datos que te pidamos, incluidos aquellos datos de salud que sean imprescindibles para poder tramitar tu matrícula en el centro de enseñanza, así como el ejercicio de la función docente y orientadora. Si no nos facilitas todos los datos que te pidamos no podremos formalizar tu matriculación en el centro de enseñanza, ya que todos ellos son necesarios para la gestión y mantenimiento de la relación del centro con sus alumnos y alumnas.

Finalmente, te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del alumno o alumna.

2.3. Padres, madres y representantes legales

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Sus datos de carácter personal recogidos a través del Formulario de Matriculación y cualesquier otros documentos que pudieran serle solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar la matrícula de su hijo, hija o menor cuya representación legal ostenta, en el centro de enseñanza, así como el ejercicio de la función docente y orientadora. Asimismo, los destinatarios de sus datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley, de conformidad con lo establecido en el artículo 11.2.a) LOPD.
b) Todos los datos solicitados a través del Formulario de Solicitud de Matriculación son de cumplimentación obligatoria.
c) De igual manera, usted consiente expresamente para el tratamiento y/o cesión de todos aquellos datos referentes a su salud necesarios para tramitar la matrícula de su hijo, hija o menor cuya representación legal ostenta en el centro de enseñanza, conforme a lo establecido en la legislación vigente.
d) Su negativa a suministrar los datos solicitados implica la imposibilidad de formalizar la matriculación de su hijo, hija o menor cuya representación legal ostenta, en el centro de enseñanza, pues son necesarios para la gestión y mantenimiento de la relación del centro con los padres, madres y representantes legales de sus alumnos y alumnas.
e) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
f) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre y de la madre o del representante legal.

2.4. Modelo simplificado alumnado menor de 14 años y familiares o representantes

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, les informamos que los datos de carácter personal recogidos a través del Formulario de Matriculación y cualesquier otros documentos que pudieran serle solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con la finalidad de tramitar la matrícula en el centro de enseñanza. Los destinatarios de los datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley. De igual manera, consienten expresamente para el tratamiento y/o cesión de todos aquellos datos de salud necesarios para tramitar la matrícula. Pueden ejercer los derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

2.5. Modelo simplificado alumnado mayor de 14 años

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu matrícula en el centro de enseñanza, así como el ejercicio de la función docente y orientadora. Asimismo, te informamos de que también necesitaremos dar a conocer tus datos a otras personas y entidades, entre las cuales estarían [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión]. Te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

3. Modelos de cláusulas legales a incorporar en los Formularios de Solicitud de Beca

3.1. Alumnado menor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Los datos de carácter personal de su hijo, hija o menor cuya representación legal ostenta, recogidos a través del Formulario de Solicitud de Beca y cualesquier otros documentos que pudieran serle solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar su solicitud de beca de estudios. Asimismo, los destinatarios de sus datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley, de conformidad con lo establecido en el artículo 11.2.a) LOPD.
b) Todos los datos solicitados a través del Formulario de Solicitud de Beca son de cumplimentación obligatoria.
c) De igual manera, usted consiente expresamente para el tratamiento y/o cesión de todos aquellos datos de salud de su hijo, hija o menor cuya representación legal ostenta, necesarios para tramitar su solicitud de beca de estudios, conforme a lo establecido en la legislación vigente.
d) Su negativa a suministrar los datos solicitados implica la imposibilidad de tramitar la solicitud de beca de estudios de su hijo, hija o menor cuya representación legal ostenta, pues son necesarios conforme a lo establecido en la legislación sectorial vigente.
e) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
f) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre, madre o representante legal.

3.2. Alumnado mayor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu solicitud de beca de estudios.

Asimismo, te informamos de que, para poder tramitar tu solicitud de beca de estudios, también necesitaremos dar a conocer tus datos a otras personas y entidades, entre las cuales estarían [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión].

Necesitaremos que nos facilites todos los datos que te pidamos, incluidos aquellos datos de salud que sean imprescindibles para poder tramitar tu solicitud de beca de estudios. Si no nos facilitas todos los datos que te pidamos no podremos tramitar tu solicitud, ya que todos ellos son necesarios para la gestión de la beca de estudios.

Finalmente, te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del alumno o alumna.

3.3. Padres, madres y representantes legales

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Sus datos de carácter personal, recogidos a través del Formulario de Solicitud de Beca y cualesquier otros documentos que pudieran serle solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar la solicitud de beca de estudios de su hijo, hija o menor cuya representación legal ostenta. Asimismo, los destinatarios de sus datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley, de conformidad con lo establecido en el artículo 11.2.a) LOPD.
b) Todos los datos solicitados a través del Formulario de Solicitud de Beca son de cumplimentación obligatoria.
c) De igual manera, usted consiente expresamente para el tratamiento y/o cesión de todos aquellos datos referentes a su salud necesarios para tramitar la solicitud de beca de estudios de su hijo, hija o menor cuya representación legal ostenta, conforme a lo establecido en la legislación vigente.
d) Su negativa a suministrar los datos solicitados implica la imposibilidad de tramitar la solicitud de beca de estudios de su hijo, hija o menor cuya representación legal ostenta, pues son necesarios conforme a lo establecido en la legislación sectorial vigente.
e) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
f) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre y de la madre o del representante legal.

3.4. Modelo simplificado alumnado menor de 14 años y familiares o representantes

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, les informamos que los datos de carácter personal recogidos a través del Formulario de Solicitud de Beca y cualesquier otros documentos que pudieran serle solicitados, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con la finalidad de tramitar la solicitud de beca de estudios. Los destinatarios de los datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley. De igual manera, consienten expresamente para el tratamiento y/o cesión de todos aquellos datos de salud necesarios para tramitar la solicitud de beca de estudios. Pueden ejercer los derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

3.5. Modelo simplificado alumnado mayor de 14 años

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu solicitud de beca de estudios. Asimismo, te informamos de que también necesitaremos dar a conocer tus datos a otras personas y entidades, entre las cuales estarían [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión]. Te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

4. Modelos de cláusulas legales a incorporar en las Fichas de jefatura de estudios

4.1. Alumnado menor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Los datos de carácter personal de su hijo, hija o menor cuya representación legal ostenta, recogidos a través de la Ficha de jefatura de estudios, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es el ejercicio de la función docente y orientadora por parte del centro de enseñanza. Asimismo, los destinatarios de sus datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley, de conformidad con lo establecido en el artículo 11.2.a) LOPD.
b) Todos los datos solicitados a través de la Ficha de jefatura de estudios son de cumplimentación obligatoria.
c) De igual manera, usted consiente expresamente para el tratamiento y/o cesión de todos aquellos datos de salud de su hijo, hija o menor cuya representación legal ostenta, necesarios para el ejercicio de la función docente y orientadora por parte del centro de enseñanza, conforme a lo establecido en la legislación vigente.
d) Los datos solicitados son necesarios para el ejercicio de la función docente y orientadora por parte del centro de enseñanza.
e) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
f) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre, madre o representante legal.

4.2. Alumnado mayor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para el ejercicio de la función docente y orientadora por parte del centro de enseñanza.

Asimismo, te informamos de que, para el ejercicio de la función docente y orientadora por parte del centro de enseñanza, también necesitaremos dar a conocer tus datos a otras personas y entidades, entre las cuales estarían [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión].

Necesitaremos que nos facilites todos los datos que te pidamos, incluidos posibles datos de salud, ya que todos ellos son necesarios para el ejercicio de la función docente y orientadora por parte del centro de enseñanza.

Finalmente, te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del alumno o alumna.

4.3. Padres, madres y representantes legales

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Sus datos de carácter personal recogidos a través de la Ficha de jefatura de estudios, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es el ejercicio de la función docente y orientadora por parte del centro de enseñanza. Asimismo, los destinatarios de sus datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley, de conformidad con lo establecido en el artículo 11.2.a) LOPD.
b) Todos los datos solicitados a través de la Ficha de jefatura de estudios son de cumplimentación obligatoria.
c) Los datos solicitados son necesarios para el ejercicio de la función docente y orientadora por parte del centro de enseñanza.
d) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
e) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre y de la madre o del representante legal.

4.4. Modelo simplificado alumnado menor de 14 años y familiares o representantes

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, les informamos que los datos de carácter personal recogidos a través de la Ficha de jefatura de estudios, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con la finalidad del ejercicio de la función docente y orientadora por parte del centro de enseñanza. Los destinatarios de los datos serán [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión], así como cualquier Administración Pública o entidad cuya cesión esté autorizada en una Ley. De igual manera, consienten expresamente para el tratamiento y/o cesión de todos aquellos datos de salud necesarios para el ejercicio de la función docente y orientadora. Pueden ejercer los derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

4.5. Modelo simplificado alumnado mayor de 14 años

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para el ejercicio de la función docente y orientadora por parte del centro de enseñanza. Asimismo, te informamos de que también necesitaremos dar a conocer tus datos a otras personas y entidades, entre las cuales estarían [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan], con la finalidad de [Indicar la finalidad a la que se destinarán los datos objeto de cesión]. Te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

5. Modelos de cláusulas legales a incorporar en los Formularios de Inscripción en las Actividades Extraescolares

5.1. Alumnado menor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Los datos de carácter personal de su hijo, hija o menor cuya representación legal ostenta, recogidos a través del Formulario de Inscripción en las Actividades Extraescolares del centro de enseñanza, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar la inscripción de su hijo, hija o menor cuya representación legal ostenta, en las Actividades Extraescolares del centro de enseñanza. Asimismo, los destinatarios de sus datos serán las terceras empresas encargadas del desarrollo e impartición de las actividades extraescolares del centro de enseñanza: [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan].
b) Todos los datos solicitados a través del Formulario de Inscripción en las Actividades Extraescolares son de cumplimentación obligatoria.
c) Su negativa a suministrar los datos solicitados implica la imposibilidad de tramitar la inscripción de su hijo, hija o menor cuya representación legal ostenta, en las Actividades Extraescolares del centro de enseñanza, pues son necesarios para la gestión de las mismas.
d) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
e) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre, madre o representante legal.

5.2. Alumnado mayor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu inscripción en las Actividades Extraescolares del centro de enseñanza.

Asimismo, te informamos de que, tramitada tu inscripción, necesitaremos dar a conocer tus datos a otras personas y entidades, encargadas del desarrollo e impartición de las actividades extraescolares del centro de enseñanza: [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan].

Necesitaremos que nos facilites todos los datos que te pidamos, incluidos aquellos datos de salud que sean imprescindibles para poder tramitar tu inscripción en las Actividades Extraescolares del centro de enseñanza. Si no nos facilitas todos los datos que te pidamos no podremos tramitar tu solicitud, ya que todos ellos son necesarios para tu inscripción en las Actividades Extraescolares del centro de enseñanza.

Finalmente, te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del alumno o alumna.

5.3. Modelo simplificado alumnado menor de 14 años y familiares o representantes

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, les informamos que los datos de carácter personal recogidos a través del Formulario de Inscripción en las Actividades Extraescolares, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con la finalidad de tramitar la inscripción en las Actividades Extraescolares del centro de enseñanza. Los destinatarios de sus datos serán las terceras empresas encargadas del desarrollo e impartición de las actividades extraescolares del centro de enseñanza: [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan]. Pueden ejercer los derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

5.4. Modelo simplificado alumnado mayor de 14 años

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu inscripción en las Actividades Extraescolares del centro de enseñanza. Asimismo, te informamos de que, tramitada tu inscripción, necesitaremos dar a conocer tus datos a otras personas y entidades, encargadas del desarrollo e impartición de las actividades extraescolares del centro de enseñanza: [Nombre de todos los posibles destinatarios de los datos y tipo de actividad que desarrollan]. Te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

6. Modelos de cláusulas legales a incorporar en los Formularios de Solicitud de Plaza en el Comedor Escolar

6.1. Alumnado menor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Los datos de carácter personal de su hijo, hija o menor cuya representación legal ostenta, recogidos a través del Formulario de Solicitud de Plaza en el Comedor Escolar, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar la solicitud de plaza de su hijo, hija o menor cuya representación legal ostenta, en el comedor escolar del centro de enseñanza. Asimismo, la empresa prestadora del servicio de comedor escolar será destinataria de sus datos: [Nombre del destinatario de los datos y tipo de actividad que desarrolla].
b) Todos los datos solicitados a través del Formulario de Solicitud de Plaza en el Comedor Escolar son de cumplimentación obligatoria.
c) De igual manera, usted consiente expresamente para el tratamiento y/o cesión de todos aquellos datos sobre posibles alergias a determinados alimentos de su hijo, hija o menor cuya representación legal ostenta, necesarios para tramitar su solicitud de plaza en el comedor escolar del centro de enseñanza.
d) Su negativa a suministrar los datos solicitados implica la imposibilidad de tramitar la solicitud de plaza de su hijo, hija o menor cuya representación legal ostenta, en el comedor escolar del centro de enseñanza, pues son necesarios para la gestión del citado servicio.
e) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
f) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre, madre o representante legal.

6.2. Alumnado mayor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu solicitud de plaza en el comedor escolar del centro de enseñanza.

Asimismo, te informamos de que, tramitada tu inscripción, necesitaremos dar a conocer tus datos a la empresa prestadora del servicio de comedor escolar: [Nombre del destinatario de los datos y tipo de actividad que desarrolla].

Necesitaremos que nos facilites todos los datos que te pidamos, incluidos aquellos datos de salud que sean imprescindibles para poder tramitar tu solicitud de plaza en el comedor escolar del centro de enseñanza. Si no nos facilitas todos los datos que te pidamos no podremos tramitar tu solicitud, ya que todos ellos son necesarios para la gestión de tu plaza en el comedor escolar del centro de enseñanza.

Finalmente, te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del alumno o alumna.

6.3. Modelo simplificado alumnado menor de 14 años y familiares o representantes

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, les informamos que los datos de carácter personal recogidos a través del Formulario de Solicitud de Plaza en el Comedor Escolar, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con la finalidad de tramitar la solicitud de plaza en el comedor escolar del centro de enseñanza. La empresa prestadora del servicio de comedor escolar será destinataria de sus datos: [Nombre del destinatario de los datos y tipo de actividad que desarrolla]. De igual manera, consienten expresamente para el tratamiento y/o cesión de todos aquellos datos sobre posibles alergias a determinados alimentos necesarios para tramitar la solicitud de plaza en el comedor escolar. Pueden ejercer los derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

6.4. Modelo simplificado alumnado mayor de 14 años

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu solicitud de plaza en el comedor escolar del centro de enseñanza. Asimismo, te informamos de que, tramitada tu inscripción, necesitaremos dar a conocer tus datos a la empresa prestadora del servicio de comedor escolar: [Nombre del destinatario de los datos y tipo de actividad que desarrolla]. Te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

7. Modelos de cláusulas legales a incorporar en los Formularios de Solicitud del servicio de transporte escolar

7.1. Alumnado menor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de los siguientes extremos:

a) Los datos de carácter personal de su hijo, hija o menor cuya representación legal ostenta, recogidos a través del Formulario de Solicitud del servicio de transporte escolar, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. La finalidad del tratamiento es la de tramitar la solicitud de su hijo, hija o menor cuya representación legal ostenta, del servicio de transporte escolar. Asimismo, la empresa prestadora del servicio de transporte escolar será destinataria de sus datos: [Nombre del destinatario de los datos y tipo de actividad que desarrolla].
b) Todos los datos solicitados a través del Formulario de Solicitud del servicio de transporte escolar son de cumplimentación obligatoria.
c) Su negativa a suministrar los datos solicitados implica la imposibilidad de tramitar la solicitud de su hijo, hija o menor cuya representación legal ostenta, del servicio de transporte escolar, pues son necesarios para la gestión del citado servicio.
d) Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
e) El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del padre, madre o representante legal.

7.2. Alumnado mayor de 14 años

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu solicitud del servicio de transporte escolar.

Asimismo, te informamos de que, tramitada tu inscripción, necesitaremos dar a conocer tus datos a la empresa prestadora del servicio de transporte escolar: [Nombre del destinatario de los datos y tipo de actividad que desarrolla].

Necesitaremos que nos facilites todos los datos que te pidamos, incluidos aquellos datos de salud que sean imprescindibles para poder tramitar tu solicitud del servicio de transporte escolar. Si no nos facilitas todos los datos que te pidamos no podremos tramitar tu solicitud, ya que todos ellos son necesarios para la gestión del servicio de transporte escolar.

Finalmente, te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

Firma del alumno o alumna.

7.3. Modelo simplificado alumnado menor de 14 años y familiares o representantes

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, les informamos que los datos de carácter personal recogidos a través del Formulario de Solicitud del servicio de transporte escolar, serán objeto de tratamiento en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con la finalidad de tramitar la solicitud del servicio de transporte escolar. La empresa prestadora del servicio de transporte escolar será destinataria de sus datos: [Nombre del destinatario de los datos y tipo de actividad que desarrolla]. Pueden ejercer los derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía. Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

7.4. Modelo simplificado alumnado mayor de 14 años

De acuerdo con la Ley de Protección de Datos de Carácter Personal, te informamos de que tus datos personales van a ser guardados y utilizados por la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía para poder tramitar tu solicitud del servicio de transporte escolar. Asimismo, te informamos de que, tramitada tu inscripción, necesitaremos dar a conocer tus datos a la empresa prestadora del servicio de transporte escolar: [Nombre del destinatario de los datos y tipo de actividad que desarrolla]. Te recordamos que tienes derecho a saber, en cualquier momento, qué datos personales tuyos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado (por ejemplo, tu dirección), o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberás dirigirte por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

8. Modelos para prestar el consentimiento para la publicación de datos de carácter personal del alumnado en la página web del centro de enseñanza

8.1. Modelo para prestar el consentimiento para el alumnado menor de 14 años

CONSENTIMIENTO PARA LA PUBLICACIÓN DE DATOS DE CARÁCTER PERSONAL DEL ALUMNO O ALUMNA EN LA PÁGINA WEB DEL CENTRO

D./Dña……....., con DNI……, en su condición de padre/madre/representante legal del alumno o alumna D./ Dña…..……, con DNI…… y domicilio en……....……...,

De conformidad con lo establecido en el art. 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal,

CONSIENTE EXPRESAMENTE

A la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla, a proceder a la publicación de los datos de carácter personal referidos a su [Indicar las categorías de datos que se quieren publicar en la página web del centro] de su hijo/a o menor cuya representación legal ostenta en la página web del centro de enseñanza, con la exclusiva finalidad de [Indicar la finalidad legítima para la cual se quieren publicar los datos de carácter personal del alumno].
Dicho consentimiento podrá ser revocado cuando exista causa justificada para ello.
De igual manera, reconoce haber sido informado de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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 y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

El responsable del citado tratamiento es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

En……, a…… de…… de……

Firma del padre, madre o representante legal.

8.2. Modelo para prestar el consentimiento para el alumnado mayor de 14 años

CONSENTIMIENTO PARA LA PUBLICACIÓN DE DATOS DE CARÁCTER PERSONAL DEL ALUMNO O ALUMNA EN LA PÁGINA WEB DEL CENTRO

Nombre y apellidos del alumno o alumna:

…….....

.....

De acuerdo con la Ley de Protección de Datos de Carácter Personal y como alumno o alumna del centro de enseñanza [Nombre del centro de enseñanza],

☐ QUIERO

☐ NO QUIERO

Que la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía publique mis datos personales sobre [Indicar las categorías de datos que se quieren publicar en la página web del centro] en la página web del centro de enseñanza donde estudio, para [Indicar la finalidad legítima para la cual se quieren publicar los datos de carácter personal del alumno].

Tengo derecho a saber, en cualquier momento, qué datos personales míos guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado, o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberé dirigirme por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

En……, a…… de…….....… de……

Firma del alumno o alumna.

ANEXO II

MODELOS ORIENTATIVOS DE CLÁUSULAS LEGALES PARA EL TRATAMIENTO DE IMÁGENES DEL ALUMNADO

1. Modelos de cláusulas legales para el tratamiento de imágenes del alumnado a través de sistemas de cámaras o videocámaras

1.1. Modelo de distintivo informativo a que se refiere el apartado 1 del ANEXO de la INSTRUCCIÓN 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras

Según establece el apartado 1 del ANEXO de la INSTRUCCIÓN 1/2006, de 8 de noviembre, *"el distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la "LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS", incluirá una mención a la finalidad para la que se tratan los datos ("ZONA VIDEOVIGILADA"), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal"*. La propia Agencia Española de Protección de Datos ha generado un modelo de distintivo informativo (ver Fig. 1) que puede ser descargado desde el Sitio Web de la AEPD.

Modelo a que se refiere el apartado 1 del ANEXO
de la INSTRUCCIÓN 1/2006

Antes de imprimir el Modelo, deben cumplimentarse los campos en blanco con el nombre del Responsable del Fichero y la dirección donde el interesado puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

1.2. Modelo de Cláusula Informativa a que se refiere el art. 3, apartado b) de la INSTRUCCIÓN 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras

De conformidad con lo dispuesto en el art. 5.1 L.O. 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado [Nombre del Fichero] del que es responsable la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, creado por Resolución [Fecha de la Resolución y Diario Oficial donde fue publicada] y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.
2. Que el destinatario de sus datos personales es [Nombre del destinatario o destinatarios de las imágenes recogidas].
3. Que puede ejercitar sus derechos de acceso, cancelación y oposición ante el responsable del fichero.
4. Que el responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, ubicado en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

1.3. Modelo de aviso informativo en cumplimiento de lo establecido en la Norma Tercera de la INSTRUCCIÓN 1/1996, de 1 de marzo, de la Agencia Española de Protección de Datos

INFORMACIÓN EN CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en los arts. 5 y 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Norma Tercera de la Instrucción 1/1996, de 1 de marzo, de la Agencia Española de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios, le informamos de la existencia de un fichero automatizado, cuya finalidad es controlar el acceso a este edificio.

Las imágenes obtenidas son las estrictamente necesarias para cumplir la finalidad de controlar el acceso. Las mismas no serán utilizadas para otros fines ni serán objeto de cesión fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Asimismo, le informamos de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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, y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

El responsable del fichero es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana, 41071, Sevilla.

2. Modelos para prestar el consentimiento para la publicación de imágenes del alumnado en la página web del centro de enseñanza

2.1. Modelo para prestar el consentimiento para el alumnado menor de 14 años

CONSENTIMIENTO PARA LA PUBLICACIÓN DE IMÁGENES DEL ALUMNO O ALUMNA EN LA PÁGINA WEB DEL CENTRO

D./Dña……....., con DNI……, en su condición de padre/madre/representante legal del alumno o alumna
D./Dña…..…….....……, con DNI…… y domicilio en……....……...,

De conformidad con lo establecido en los artículos 6.1 y 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el art. 2.2 de la 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,

CONSIENTE EXPRESAMENTE

A la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla, a proceder a la publicación de la imagen de su hijo/a o menor cuya representación legal ostenta en la página web del centro de enseñanza, con la exclusiva finalidad de [Indicar la finalidad legítima para la cual se quiere publicar la imagen del alumno].

De igual manera, reconoce haber sido informado de la posibilidad de ejercitar los correspondientes derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el 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, y en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
El responsable del citado tratamiento es la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

En……, a…… de…… de……

Firma del padre, madre o representante legal.

2.2. Modelo para prestar el consentimiento para el alumnado mayor de 14 años

CONSENTIMIENTO PARA LA PUBLICACIÓN DE IMÁGENES DEL ALUMNO O ALUMNA EN LA PÁGINA WEB DEL CENTRO

Nombre y apellidos del alumno o alumna:

…….....

De acuerdo con la Ley de Protección de Datos de Carácter Personal y la Ley de Protección de mi derecho al honor, a mi intimidad personal y familiar y a mi propia imagen y como alumno o alumna del centro de enseñanza [Nombre del centro de enseñanza],

☐ QUIERO

☐ NO QUIERO

Que la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía publique mi imagen en la página web del centro de enseñanza donde estudio, para [Indicar la finalidad legítima para la cual se quiere publicar la imagen del alumno].

Tengo derecho a saber, en cualquier momento, qué datos personales míos (incluyendo mi imagen) guarda la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía y para qué, modificarlos si éstos han cambiado, o borrarlos (en los casos en que ello fuera legalmente posible). Para ello, deberé dirigirme por escrito a la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, con dirección en Avda. Juan Antonio de Vizarrón, s/n, Edificio Torretriana. 41071, Sevilla.

En……, a…… de…… de……

Firma del alumno o alumna.

ANEXO III

CONSIDERACIONES SOBRE PROYECTOS DE MOVILIDAD PARA EL PROFESORADO EN RELACIÓN CON LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Introducción

En el presente Anexo, se analiza la incidencia de la normativa de Protección de Datos de Carácter Personal sobre el proyectos de movilidad para el profesorado, basado en la utilización de dispositivos móviles para la gestión del alumnado en los centros educativos (faltas de asistencia a actividades docentes y extraescolares, calificaciones diarias, seguimiento de conductas contrarias a la convivencia, observaciones sobre alumnos, etc.). Estos datos residen en cada dispositivo, a modo de "cuaderno del profesorado", y se sincronizan vía Internet con *Séneca* para mantener la información coherente y actualizada.

2. Análisis de la incidencia de la normativa de Protección de Datos de Carácter Personal sobre proyectos de movilidad

Como punto de partida, hemos de recordar que el artículo 10 de la LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), bajo la rúbrica general de *"Deber de secreto"*, determina que *"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*.

En este sentido, todo el profesorado que intervenga en el tratamiento de los datos de carácter personal contenidos en los ficheros responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, a través de los dispositivos móviles para la gestión del alumnado, queda sujeto al deber de secreto establecido en el art. 10 LOPD.

Asimismo, el artículo 89 del 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, relativo a las *"Funciones y obligaciones del personal"*, dispone

que *"El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento"* (art. 89.2).

De tal manera, se recomienda realizar las siguientes indicaciones al profesorado que intervenga en el tratamiento de los datos de carácter personal a través de los dispositivos móviles para la gestión del alumnado:

- Establecer la prohibición general de introducir en el dispositivo móvil cualquier información u observación que pueda contener datos de carácter personal especialmente protegidos: datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias o que hagan referencia al origen racial, a la salud y a la vida sexual del alumnado o sus familiares. De no llevarse a cabo esta recomendación, existiría la obligación de implementar todas las medidas de seguridad contempladas en el Real Decreto 1720/2007 para aquellos ficheros que contengan datos de carácter personal de nivel alto, entre las cuales cabe citar, a modo de ejemplo, el cifrado de los datos contenidos en los dispositivos móviles (art. 101.2 párrafo segundo Real Decreto 1720/2007), la implementación de un registro de accesos conforme a lo establecido en el art. 103 del Real Decreto 1720/2007 (identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado) o el cifrado de los datos cuando sean transmitidos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas con destino a Séneca (art. 104 Real Decreto 1720/2007).

- Establecer la prohibición general de instalar, por propia iniciativa, cualquier aplicación informática en los dispositivos móviles.

- Establecer la prohibición general de utilizar los dispositivos móviles para uso privado o cualquier otra finalidad distinta de la gestión del alumnado en los centros educativos.

- Establecer la prohibición general de crear nuevos ficheros que contengan datos de carácter personal en los dispositivos móviles. En este sentido, la LOPD califica como infracción grave *"Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente"* (art. 44.3.a) LOPD). Asimismo, la Ley Orgánica 15/1999 establece que *"no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas"* (art. 9.2 LOPD).

- Asimismo, recordar su sujeción al *"Deber de secreto"* establecido en el art. 10 LOPD, lo cual impide al profesorado revelar o dar a conocer la información gestionada a través de los dispositivos móviles puestos a su disposición.

En cuanto a las consecuencias en que pudiera incurrir en caso de incumplimiento, señalar que será de aplicación lo dispuesto en la legislación sobre régimen disciplinario de las Administraciones Públicas (art. 45.2 LOPD).

Por otro lado, el artículo 86 del Real Decreto 1720/2007, dedicado al *"Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento"*, establece lo siguiente: *"Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado"* (art. 86.1 Real Decreto 1720/2007). Asimismo, conforme a lo establecido en el art. 86.2 del Real Decreto 1720/2007, la citada autorización deberá constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Por otro lado, a efectos del Real Decreto 1720/2007, se entiende por *"soporte"* el *"objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos"* (art. 5.2.ñ) Real Decreto 1720/2007). De esta definición, podemos afirmar que todos aquellos artículos del Real Decreto 1720/2007 relativos a los *"soportes"* serán aplicables a los dispositivos móviles puestos a disposición del profesorado.

En este sentido, el art. 92 del Real Decreto 1720/2007, relativo a la *"Gestión de soportes y documentos"*, señala que *"La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad"* (art. 92.2 Real Decreto 1720/2007).

Por tanto, debe establecerse, con carácter general, la prohibición para el profesorado de trabajar con los dispositivos móviles fuera de los locales del centro educativo, salvo que exista causa justificada para ello y autorización expresa de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, como responsable de los ficheros de datos de carácter personal contenidos en los mismos, para:

- La salida del centro educativo del dispositivo móvil que le ha sido facilitado por el responsable del fichero para la gestión del alumnado, en cumplimiento del art. 92.2 Real Decreto 1720/2007.

- El consiguiente tratamiento de los datos de carácter personal contenidos en el dispositivo móvil fuera de los locales del centro educativo, en cumplimiento del art. 86 Real Decreto 1720/2007.

Dicho requisito formal ha de ser inexcusable para poder trabajar con los dispositivos móviles fuera de los locales del centro educativo.

Asimismo, el art. 92.1 Real Decreto 1720/2007 establece que *"Los soportes y documentos que contengan datos de carácter personal deberán*

permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad".

En su consecuencia, deberá realizarse un inventario de los dispositivos móviles existentes en cada uno de los centros educativos que contenga, al menos, la siguiente información:

- Número de inventario que se le asigna al dispositivo móvil.

- Tipo de información que contiene (datos del alumnado, familiares, etc.).

- Nivel de seguridad asignado, en función de los datos que contenga (básico, medio o alto).

- Persona expresamente autorizada para su utilización.

- Perfil del usuario del dispositivo móvil (docente, etc.).

- Fecha de inicio y terminación, en su caso, de la utilización del dispositivo móvil para la gestión del alumnado en el centro educativo.

Asimismo, conforme a lo establecido en el art. 92.5 Real Decreto 1720/2007, deberá procederse a la identificación de cada uno de los dispositivos móviles, utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

De igual manera, el lugar donde se almacenen los dispositivos móviles debe disponer de algún mecanismo que obstaculice su apertura (por ejemplo, una cerradura con llave o un candado). Como es lógico pensar, únicamente deben disponer de una copia de la citada llave aquellas personas expresamente autorizadas para la utilización de los dispositivos móviles para la gestión del alumnado.

En el supuesto de que los dispositivos móviles contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los alumnos y alumnas del centro y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, también será de aplicación lo dispuesto en el art. 97 del Real Decreto 1720/2007 con respecto a la gestión de soportes. No obstante lo anterior, hemos de recordar que el Real Decreto 1720/2007 es una norma de *"mínimos"* (las medidas incluidas en cada uno de los niveles tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero), lo cual aconseja la implantación de lo establecido en el art. 97 Real Decreto 1720/2007 en todo caso:

"Artículo 97. Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada."

En base a lo anteriormente indicado, en cada uno de los centros educativos deberá implementarse un "Libro registro de entrada de dispositivos móviles" en el cual quede reflejada, al menos, la siguiente información:

- Tipo de soporte y número de inventario asignado.

- Fecha y hora de entrada.

- Emisor del envío (si lo hubiera).

- Tipo de información que contiene (datos del alumnado, familiares, etc.).

- Nivel de seguridad asignado, en función de los datos que contenga (básico, medio o alto).

- Forma de envío (si lo hubiera).

- Nombre, apellidos y firma de la persona expresamente autorizada para la recepción y utilización del dispositivo móvil.

De igual manera, deberá implementarse un "Libro registro de salida de dispositivos móviles" en el cual quede reflejada, al menos, la siguiente información:

- Tipo de soporte y número de inventario asignado.

- Fecha y hora de salida.

- Destinatario (si lo hubiera) del dispositivo móvil.

- Tipo de información que contiene (datos del alumnado, familiares, etc.).
- Nivel de seguridad asignado, en función de los datos que contenga (básico, medio o alto).

- Forma de envío (si lo hubiera).

- Precauciones y/o medidas de seguridad para el transporte del dispositivo móvil.

- Nombre y apellidos de la persona expresamente autorizada para

gestionar dicha salida.

- Nombre y apellidos, puesto o cargo y firma de la persona que autoriza la salida del dispositivo móvil.

Con respecto al acceso a la aplicación instalada en los dispositivos móviles para la gestión del alumnado, recordar que, conforme a lo establecido en el artículo 93 del Real Decreto 1720/2007, deberán implementarse las siguientes medidas de seguridad:

- Se deberá elaborar una relación actualizada del profesorado que tenga acceso autorizado a la aplicación para la gestión del alumnado instalada en los dispositivos móviles.

- Se establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel que intente acceder a la aplicación para la gestión del alumnado instalada en los dispositivos móviles y la verificación de que está autorizado.

- Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

- Las contraseñas se cambiarán periódicamente (por ejemplo, cada 180 días) y mientras estén vigentes se almacenarán de forma ininteligible. La periodicidad para el cambio de contraseñas en ningún caso podrá ser superior a un año.

- Con carácter adicional, se recomienda limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información (por ejemplo, tres intentos). Dicha medida de seguridad queda recogida en el artículo 98 del Real Decreto 1720/2007.

Finalmente, como medida de seguridad adicional, se recomienda que cuando los datos de carácter personal sean transmitidos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas con destino

a Séneca, dicha transmisión se realice a través de protocolo seguro que proporcione el cifrado de dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

La citada obligación sólo se contempla, conforme a lo establecido en el art. 104 Real Decreto 1720/2007, para aquellos casos en que se transmitan datos de nivel alto (en principio, se establece la prohibición general para el profesorado de introducir en el dispositivo móvil cualquier información u observación que pueda contener datos de carácter personal de nivel alto). Ahora bien, como hemos indicado anteriormente, el Real Decreto 1720/2007 es una norma de "mínimos" (las medidas incluidas en cada uno de los niveles tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero), lo cual aconseja la utilización de los mecanismos citados para evitar el acceso por parte de terceros no autorizados a los datos de carácter transmitidos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas con destino a Séneca.

3. Modelo de solicitud para la obtención de la autorización expresa para trabajar con los dispositivos móviles fuera de los locales del centro educativo

SOLICITUD DE AUTORIZACIÓN EXPRESA PARA TRABAJAR CON LOS DISPOSITIVOS MÓVILES FUERA DE LOS LOCALES DEL CENTRO EDUCATIVO

DON/DOÑA ....., con Documento Nacional de Identidad número ....., como usuario/usuaria de los ficheros de datos de carácter personal responsabilidad de la Secretaría General Técnica de la Consejería de Educación de la Junta de Andalucía, en el centro educativo .... ubicado en ……. ...., en cumplimiento de lo establecido en los artículos 86 y 92 del 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,

SOLICITA

La autorización expresa para la salida del centro educativo del dispositivo móvil (PDA) que le ha sido facilitado por el Responsable del Fichero para la gestión del alumnado, así como el consiguiente tratamiento de los datos de carácter personal en él contenidos fuera de los locales del mismo, con las siguientes finalidades:

☐ Utilización del dispositivo móvil, a modo de "cuaderno del profesorado", en el domicilio particular del docente.

☐ Otras finalidades (especificar): .....

.....

Dicha autorización se solicita para el siguiente período de tiempo:

☐ Año Académico: .....

☐ Otro período de tiempo (especificar): .....

.....

Las medidas de seguridad previstas para la protección de los datos de carácter personal contenidos en el dispositivo móvil son las siguientes:

- Mecanismo para la identificación de forma inequívoca y personalizada de todo aquel que intente acceder a los datos de carácter personal contenidos en el dispositivo móvil y la verificación de que está autorizado.
- Cifrado de los datos de carácter personal contenidos en el dispositivo móvil.
- Uso de protocolo seguro que proporcione el cifrado de los datos de carácter personal contenidos en el dispositivo móvil cuando sean transmitidos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas con destino a *Séneca*.

Y para que así conste, firma la presente solicitud en …….....……., a ….....de …….....de 20….....

Firma del/la solicitante