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)

Copia literal de la obra GUÍA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL PARA LOS CENTROS DE ENSEÑANZA publicada por la Consejería de Educación de la Junta de Andalucía

Isidro Gómez-Juárez Sidera.

Experto en Protección de Datos de Carácter Personal.
DEA en Derecho de las Nuevas Tecnologías de la Información y las Comunicaciones.

Secretaría General Técnica de la Consejería de Educación

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

Secretaría General Técnica

ISBN: 978-84-690-6607-2

Aviso importante:

Índice

I. EL DERECHO A LA PROTECCIÓN DE DATOS DE CARACTER PERSONAL

En España, el derecho a la protección de datos de carácter personal tiene, desde la Sentencia del Tribunal Constitucional 292/2000, de 20 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 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.

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.

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.

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

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

1.1. 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.

  http://europa.eu/legislation_summaries/information_society/%20l14012_es.htm

1.2. Normativa nacional general

- LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

  https://www.boe.es/buscar/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.

  https://www.boe.es/buscar/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 428/1992, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

1.3. Normativa nacional y autonómica sectorial

- Disposición adicional vigesimotercera de la LEY ORGÁNICA 2/2006, de 3 de mayo, de Educación.

  https://www.boe.es/diario_boe/txt.php?id=BOE-A-2006-7899

- Disposición adicional segunda de la LEY 17/2007, de 10 de diciembre, de Educación de Andalucía.

  https://www.juntadeandalucia.es/boja/2007/252/1

- 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.

  https://www.juntadeandalucia.es/boja/2010/91/20

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.

Asimismo, el 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 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 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 de 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. 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.

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 un 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 mismo se recaben para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias (la actividad prestaciones de educación en el caso de un centro educativo público).

Asimismo, la Disposición adicional vigesimotercera 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 plante la Disposición adicional vigesimotercera de la LOE queda limitada exclusivamente a la "función docente y orientadora" del centro, no pudiendo tratarse los datos del alumno con fines diferentes del educativo sin el consentimiento expreso de los mismos/as o de sus padres, madres o representantes legales, según proceda.

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 Real Decreto 1720/2007, de 21 de diciembre, 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 que 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. 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*".

Esto es, la ley Orgánica 15/1999 establece en su art. 19 un deber de secreto para todo aquél o aquella que tenga acceso a los datos de carácter personal gestionados en el centro en el desempeño de sus funciones.

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.

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

1. Recomendaciones sobre protección de la documentación en soporte papel

1.1. 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.

Nivel Medio

La adopción de las medidas de seguridad de nivel medio sólo será necesaria en aquellos supuestos que el fichero en cuestión contenga un conjunto de datos de carácter personal que ofrezcan una definición de 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.

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).

Nivel Alto

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.

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.

1.2. Medidas de seguridad

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 aquellas recogidas en los niveles inferiores.

Nivel Básico

- Cada una de las personas que trabajan en el centro de enseñanza deben tener perfectamente delimitadas su funciones y obligaciones, de tal manera que solo tengan acceso a aquellos documentos imprescindibles para el ejercicio de su actividad concreta, ya sea personal docente, de administración, servicios o cualquier otro.
- 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 archivados 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.

- 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 encarguen 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 1729/2007, 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 y 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 contenido 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 del 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 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.

2. 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 que 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.

Frente a la 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 confidenciales 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. 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 la 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 será 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 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 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 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.
- Nivel 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, 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 en archivo en papel de la Administración General del Estado hace referencia al tema de las garantías en caso de que se contrate una empresa especializadas 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 presencia 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 video es positiva, es interesante que cuanto menos en alguna ocasión esté presente un responsable del centro cuya documentación está siendo objeto de destrucción, a fin de presenciar el proceso in situ.

Asimismo, resaltar la importación 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 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 procesaos 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).

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

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

1.1. 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, patio, 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.

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, 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)).

1.2. 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*".

1.3. 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.

1.4. Aplicación de los principios de protección de datos conforme a los 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 publicada en Portal Séneca).

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 publicada en Portal Séneca).

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

La difusión de las Tecnologías de la Información y las Comunicaciones (TIC's) 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).

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.

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 publicada en Portal Séneca), 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 publicada en Portal Séneca), que sirvan de utilidad a los centros de enseñanza.

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

1. 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"*.

2. ¿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.

3. 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 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.

4. 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?

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.

5. ¿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.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*".

6. 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.

7. ¿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?

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 grave en el artículo 44.3.d) 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 siendo igualmente aplicable el art. 44.3.d) 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) podríamos llegar a encontrarnos ante una infracción muy grave aplicando el artículo 44.4.b) de la LOPD.

8. ¿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.

9. ¿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?

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 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. 46.2 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.

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