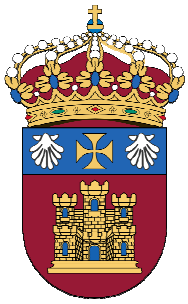
# “IMPLANTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS APLICADA A COLEGIOS PÚBLICOS Y PRIVADO-CONCERTADOS DE CASTILLA Y LEÓN”



Autor del proyecto: *D. Ángel Gañán Adánez*
Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez
Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosio

MAGÍSTER EN ASESORÍA Y CONSULTORÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
(MAC-TIC)

UNIVERSIDAD DE BURGOS
II Edición. Burgos, Septiembre 2010.

***Magíster financiado por la Fundación Centro de Supercomputación de Castilla y León***

AGRADECIMIENTOS

No quiero comenzar este trabajo sin antes agradecer a todas las personas que de una u otra forma se han implicado en él apoyándome de manera incondicional. También debo agradecer a todos mis profesores el esfuerzo y dedicación con el que desempeñaron su tarea docente, especialmente en estos momentos en los que ejerzo la profesión y conozco desde dentro la entrega que exige el contacto directo con los alumnos.

De manera especial quiero expresar mi más sincero agradecimiento a los Directores del Magister Dr. Emilio S. Corchado Rodríguez y el Dr. Álvaro Herrero Cosio, al Tutor y Profesor del Proyecto Miguel Ángel Davara Rodríguez, al Profesor Emilio Montoya, a la Profesora Elena Davara y al resto de Profesores y compañeros de clase, por su disponibilidad y atención constantes, así como sus recomendaciones y aclaraciones durante el curso académico para que este trabajo pudiera ser elaborado y terminado, a todos ellos/a gracias.

Mi agradecimiento y dedicatoria final va dedicado a mi familia y a Marta por sus infatigables esfuerzos, por su aguante y por el apoyo dado durante la realización del trabajo.

Introducción

Somos muchos los que nos hemos preguntado alguna vez si aquellos que tratan nuestros datos personales no tendrán demasiada información sobre nuestra vida privada y cotidiana. Es obvio que debe existir un control sobre nuestros datos personales para que podamos sentirnos protegidos.

Los datos de personas, que no son cosas, y que tienen una natural dignidad, y por tanto tienen derecho a ser tratadas como tales: a que se respete su condición, a saber qué se está haciendo con su nombre, a saber qué se está haciendo con sus datos personales… en una palabra, a la intimidad.

La Ley sobre Protección de Datos de Carácter Personal (LOPD) establece un límite sobre la tenencia y utilización de este tipo de datos así como sobre el tráfico de los mismos. De esta manera, la Agencia de Protección de Datos se encarga de facilitar al ciudadano el derecho a conocer quién está utilizando sus datos personales y para qué, y negar el permiso sobre el uso de sus datos a quien nosotros consideremos oportuno.

Con este trabajo, se persigue realizar el proyecto fin de Magíster en Asesoría y Consultoría en Tecnologías de la Comunicación y las Telecomunicaciones.

Este proyecto se basará en la implantación de la Ley de Protección de Datos en Centros escolares de Educación Primaria en la Comunidad de Castilla y León en los Centros Públicos cómo en los Centros Privados Concertados. Los ámbitos que se tratarán en el trabajo son ley orgánica de protección de datos, la ley de comercio electrónico, la fiscalidad electrónica y administración, firma electrónica, el documento de seguridad, las medidas de seguridad, procedimiento de recuperación de dominio, propiedad intelectual (derechos patrimoniales y morales), contratos informáticos (contratos de adhesión).

Por otra parte, se realizará un pequeño análisis de la situación actual de la aplicación de la ley de protección de datos en los centros escolares para poder tener en cuenta a la hora de plantear la implantación de la LOPD en los centros escolares además de sensibilizar al sector sobre el necesario cumplimiento de la normativa de protección de datos que de manera repetida se incumple, generalmente debido al desconocimiento de ésta. Pretendemos así

evitar  posibles infracciones que pudieran producirse y las temidas sanciones tanto de carácter administrativo como de carácter económico.

**Glosario de abreviaturas**

AEPD: Agencia Española de Protección de Datos

Art.: Artículo

AECE: Asociación Española de Comercio Electrónico

AEAT: Agencia Estatal de la Administración Tributaria

ASPs: Application Service Providers

B2A: Business to Administration

B2B: Business to Business

B2C: Business to Consumer

BOE: Boletín Oficial del Estado

BOCYL: Boletín Oficial de Castilla y León

CEE: Comunidad económica Europea

C2C: Consumer to consumer

CGC: Condiciones Generales de Contratación

CIF: Código de Identificación Fiscal

DNS: Domain Name Service

EE. UU.: Estados Unidos

ES: España

FNMT-RCM: Fábrica Nacional de Moneda y Timbre

INE: Instituto Nacional de Estadística

IP: Internet Protocol

IVA: Impuesto sobre el valor añadido

JCYL: Junta de Castilla y León

LOPD: Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos Personales

LORTAD: Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

LSSI: Ley de Servicios de la Sociedad de la Información

OCDE: Organization for Economic Cooperation and Development (Organización de Cooperación y Desarrollo).

OMC: Organización Mundial de Comercio

OMPI/WIPO: Organización Mundial de la Propiedad Intelectual

RD: Real Decreto

RR. HH.: recursos humanos

# Índice temático

## 1.1 Datos de carácter personal, ficheros y “bases de datos”

Como se indica en el artículo 3 de la ley 15/1999 de Protección de Datos de carácter personal se conceptualiza algunas definiciones de suma importancia a la hora de tratar datos de carácter personal como son:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
g) Encargado del tratamiento: 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.
h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

Los “ficheros” que afectan a la vida de las personas, y que “tratan” información de carácter personal, han existido desde siempre, sólo que en papel.
Dentro de los ficheros podemos distinguir dos tipos en función de la titularidad de los mismos, pudiéndose ser de titularidad pública en el que el responsable es una administración pública y los ficheros de titularidad privada en los que el titular es una empresa o entidad. En

el trabajo que nos ocupa trataremos con ficheros de titularidad privada y pública ya que son centros públicos y centros privados concertados en los que parte de los ficheros son de carácter privado.

El cambio que opera la informática es que multiplica para cualquier organización o persona la posibilidad de realizar un tratamiento automático y racional de la información. Ésta se encuentra recogida en archivos informáticos llamados
"bases de datos", que sustituyen a los antiguos ficheros de papel. Estos archivos informáticos, las bases de datos, son también ficheros. Lo único que cambia es el formato: son ficheros (archivos) informáticos.

La mayor potencia de los ordenadores sobre el papel a la hora de "tratar" la información que suministran las bases de datos, y la generalización de su uso por cualquiera que tenga un PC, ha obligado a los gobiernos a publicar normas jurídicas que regulen el tratamiento de la información. Ya en 1951 se creó en Estados Unidos la "Oficina Intergubernamental para la informática" (I.B.I). Este organismo ya ponía de manifiesto la influencia que tiene la Informática en la sociedad y que los países deberían de disponer de mecanismos para facilitar el uso de la misma y contribuir al bienestar de la humanidad en su contexto cultural, económico y social.

En el caso que nos ocupa, en España la LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y 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 legislan lo concerniente al tratamiento de los datos de carácter personal.

A la hora de realizar el trabajo tendremos en cuenta también la legislación educativa que encontramos en la LEY ORGÁNICA 2/2006, de 3 de mayo, de Educación, ORDEN EDU/1951/2007, de 29 de noviembre, por la que se regula la evaluación en la educación primaria en Castilla y León que hacen referencia la Ley Orgánica de Protección de Datos de Carácter Personal.

Hay que tener presente que la LOE recoge dos asuntos de especial incidencia en relación al presente Plan de Oficio. Por un lado, en su artículo 120, reconoce el principio de autonomía organizativa, pedagógica y de gestión de los centros docentes, aunque las Administraciones deban establecer el marco general en que deba desenvolverse la actividad educativa, y, por otro, recoge, en su disposición adicional vigésimo tercera, un apartado referente a los datos personales de los alumnos, en virtud del cual los centros escolares podrán recabar sus datos para el ejercicio de la función educativa, siempre que sea la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse para fines diferentes del educativo sin consentimiento expreso.

Por otra parte, tendremos en cuenta el **Real Decreto** Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la **Ley** de Propiedad Intelectual, la **LEY** 59/2003, de 19 de diciembre, de firma electrónica, la **LEY** 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

### 1.1.1 Identificación de los ficheros

Las empresas y profesionales, para el desarrollo normal de la actividad que les es propia, requieren manejar datos de carácter personal. Sus diferentes áreas funcionales -departamento de compras, ventas, marketing, contabilidad, personal, etc.- cuentan con ficheros creados con diversas finalidades.
Estos datos suelen almacenarse en "ficheros" o bases de datos. La LORD define a los ficheros como todo conjunto organizado de datos de carácter personal, con independencia de la forma o modalidad de creación, almacenamiento, organización y acceso. Pueden figurar en soporte de papel (archivos o ficheros manuales) o estar informatizados en una base de datos (fichero automatizado).
Desde la entrada en vigor de la LORD también son objeto de regulación los ficheros físicos, es decir, también deberán considerarse a efectos de la normativa de protección de datos de carácter personal, los ficheros no informáticos.

Generalmente encontrarnos que la mayoría de los centros educativos tienen gran parte de datos personales de alumnos en soporte papel y aunque no estuvieran informatizados también

tienen la consideración de ficheros de datos de carácter personal por lo tanto, les es de aplicación la normativa de protección de datos de carácter personal o los ficheros en soporte físico como papel.

A continuación, a título ilustrativo, se recogen algunos ejemplos de los ficheros más usuales que puede haber en el seno de una empresa:

| Nombre del fichero | Descripción | Finalidad |
|---|---|---|
| Clientes/alumnos | Datos de las personas a las que el responsable presta servicios o suministra productos | Gestión de clientes<br>Información al alumnado y padres o representantes legales<br>Actividades extraescolares realizadas en el centro |
| Proveedores | Datos de las personas de las que el responsable (Centro) recibe productos o servicios | Gestión de proveedores |
| Trabajadores | Datos de las personas que trabajan en la empresa, en la Administración o para el Profesional y que tienen acceso a datos de carácter personal | Gestión del personal. |
| Salud | Datos de salud de los trabajadores. Pueden estar incluidos en el fichero de trabajadores, pero en la mayoría de empresas o Administraciones dichos datos están en un fichero aparte o están en poder de una mutua. | Gestión de la salud |
| Usuarios | Datos de las personas que utilizan un servicio gratuito para el que es necesario registrarse. Es muy habitual en las páginas Web por ejemplo la que suelen tener abiertas los Centros Escolares. | Gestión de usuarios |

| Nombre del fichero | Descripción | Finalidad |
|---|---|---|
| Suscriptores | Datos de las personas suscritas a un boletín, revista o servicio ofertado por los centros escolares. | Gestión de suscriptores |
| Asociados | Datos de las personas que forman parte de una asociación, club u organización por ejemplo del AMPA | Gestión de asociados |
| Socios | Datos de las personas que sean socios de una empresa | Gestión de socios |
| Curriculums | Datos de las personas que han solicitado trabajar en la empresa, Administración o para un profesional y han remitido información | Selección de personal |
| Acceso a edificios | Datos de las personas que acceden a un edificio en el caso que se les identifique en la entrada | Control del acceso y medidas de seguridad |

Elaboración propia

### 1.1.2 NOTIFICACIÓN DE FICHEROS

De forma previa a la creación de cualquier fichero con datos de carácter personal, será obligatorio proceder a la notificación ante el Registro de Ficheros de la Agencia de Protección de Datos. Para notificar la creación de un fichero será necesario proceder a la cumplimentación de un formulario oficial, bien en soporte de papel bien en soporte electrónico y presentarlo ante el Registro de Ficheros de la Agencia de Protección de Datos.

En el caso de ficheros de titularidad pública como se indica en el Art. 20 de la LOPD en 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.
En el apartado 2 del artículo 20 de la LOPD indica que las disposiciones de creación o de modificación de ficheros deberán indicar:

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

En el apartado número 3 del mismo artículo se hace mención a la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

En el caso de ficheros de titularidad privada en el artículo 25 de la LOPD se indica que podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

En el artículo 26 de la LOPD se hace referencia a la notificación e inscripción registral señalando en su apartado primero que toda persona o entidad que proceda a la creación de

ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

En el apartado 2 de artículo 26 de la LOPD se señala que por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países.

### 1.1.3 Requisitos.

1.1.3.1 Conforme al Art. 25 de la LOPD, únicamente podrán crearse ficheros de titularidad privada (no pertenecientes a las Administraciones Públicas) que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad.
Los fines no son únicamente un presupuesto habilitante para la creación de ficheros privados, sino que también condicionarán la acción de recogida de los datos contenidos en él, puesto que éstos sólo podrán ser recabados si son adecuados o pertinentes para la consecución de dichos fines.

1.1.3.2Quedan prohibidos 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.

### 1.1.4 Notificación.

Este aspecto aparece regulado tanto en el Art. 26 LOPD, como en el Art. 6 del Real Decreto 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.

A continuación procedemos a explicar cómo se ha de rellenar el formulario oficial para notificar un fichero de datos de carácter personal ante la Agencia de Protección de Datos, el conocido archivo NOTA.

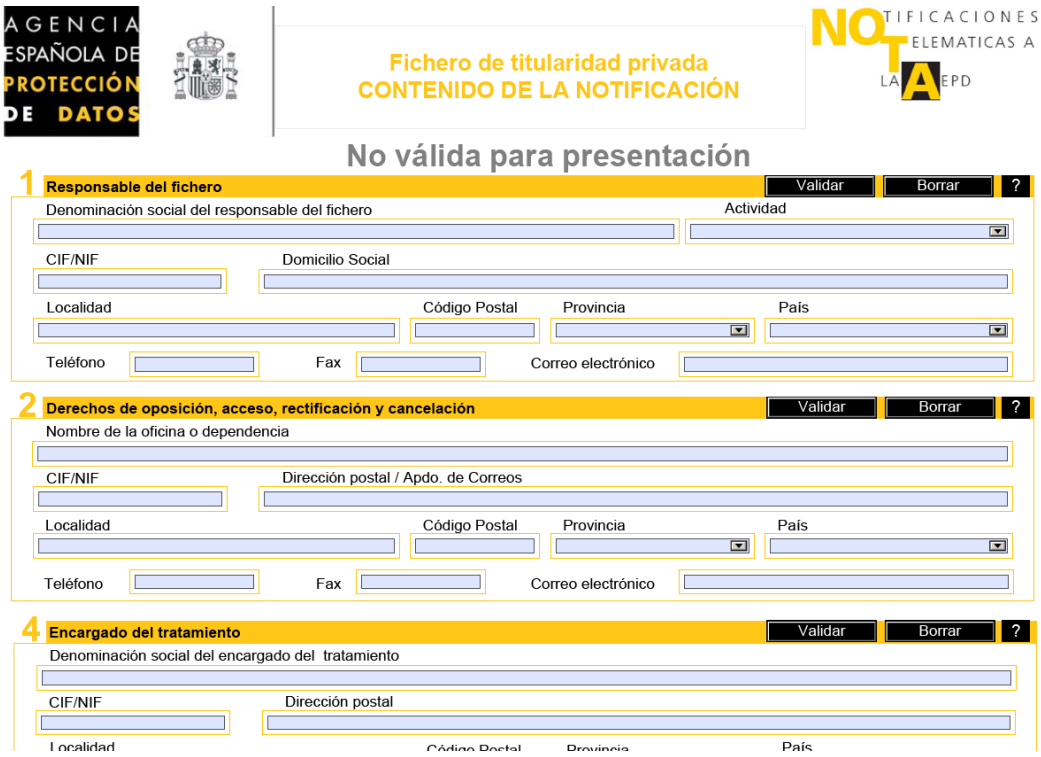
### 1.1.5 Solicitud

La primera hoja corresponde a la solicitud en la cual deberemos indicar los siguientes datos:

a) Tipo de solicitud: en función de si se trata de la inscripción, la modificación o la cancelación de un fichero marcaremos una de las tres opciones.

b) Datos de la persona física que presenta la notificación. Normalmente un representante legal de la empresa.

c) Dirección a efectos de notificación: será el lugar donde la Agencia de Protección de Datos remitirá cualquier comunicación en relación a la solicitud de inscripción.
En el siguiente cuadro podemos ver los datos requeridos en la solicitud NOTA para ficheros de titularidad privada:




Fuente: Agencia Española de Protección de Datos

### 1.1.6 Responsable del fichero o tratamiento

En este apartado se indicará la persona física o jurídica responsable del fichero, aquella que decida sobre su finalidad, contenido y tratamiento.
Los datos a consignar son los siguientes: nombre o razón social, número de identificación fiscal (NIF) o código de identificación fiscal (CIF), actividad u objeto social del responsable del fichero y la dirección. El teléfono, fax y e mail son de cumplimentación opcional.

### 1.1.7 Servicio o Unidad ante el que pueden ejercitarse los derechos de oposición, acceso, rectificación y cancelación

Las personas cuyos datos forman parte de un fichero tienen diferentes derechos que pueden ejercitar. Este apartado deberá rellenarse en el caso que la dirección en la cual puedan ejercitarse estos derechos sea diferente a la que se haya indicado para el responsable del fichero.

### 1.1.8 Ubicación principal

En este apartado se deberá informar de la ubicación real de los datos. Muchas empresas tienen sus oficinas (ubicación real de los datos) en una dirección y su domicilio social, que es el del responsable del fichero, en otra, con lo cual aquí deberá indicar la dirección de las oficinas en las que se encuentren los datos en el caso que sea diferente de la indicada para el responsable del fichero.

### 1.1.9 Encargado del tratamiento

Se deberá indicar, en el caso que exista, la persona física o jurídica que trate los datos sola o conjuntamente por cuenta del responsable del tratamiento.
Normalmente, las empresas tienen contratadas a gestorías que les realizan todos los trámites y gestiones laborales de sus trabajadores. En estos casos, deberá figurar como encargado del tratamiento del fichero de trabajadores la gestoría.

También ocurrirá lo mismo en el caso que el responsable del tratamiento entregue los datos de sus clientes o proveedores a una gestoría para que le realice todos los trámites fiscales. En estos supuestos, en los ficheros de clientes y proveedores deberá indicarse que el encargado del tratamiento es la gestoría.
Las empresas o los profesionales que almacenen u obtengan datos de carácter personal través de su página Web deberán indicar como encargada del tratamiento a la empresa que le presta los servicios de hospedaje de su página Web.

### 1.1.10 Sistemas de tratamiento o de información

Se deberá describir brevemente el conjunto de los ficheros, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal. Asimismo, deberá señalarse si el sistema de información corresponde a servidores centrales, ordenadores personales u otros. Además, se señalará si se dispone de conexiones externas y el tipo de red (corporativa, Intranet, Internet).

### 1.1.11 Medidas de seguridad

En este apartado debe indicarse el nivel de las medidas de seguridad exigibles en función de los tipos de datos.
Las medidas de seguridad aplicables a los ficheros que contengan datos de carácter personal serán de tres tipos, en función de los tipos de datos de que se disponga.

Los niveles de seguridad son:
a) Alto.
b) Medio.
c) Básico.
En el artículo 4 del Real Decreto 994/1999 se detallan cuales son los datos que se incluyen en cada nivel.

### 1.1.12 Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero

Se deben identificar los datos que integrarán el fichero de datos de carácter personal, individualizando los supuestos de datos especialmente protegidos.

Los datos especialmente protegidos sólo serán cumplimentados cuando sean objeto de tratamiento datos relativos a: la ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud y vida sexual. Además, deberán señalarse los supuestos a los que se acoge para poder tratarlos, ya que la legislación obliga para estos supuestos que el afectado haya dado su consentimiento expreso.

Se deberán señalar aquellos datos que el fichero contenga.

Es importante tener en cuenta que los datos de carácter personal sólo podrán recogerse cuando sean adecuados, pertinentes y no excesivos en relación con las finalidades del mismo.

En el caso que se esté procediendo a notificar el fichero correspondiente a los clientes, en atención a lo expuesto sólo serán pertinentes los datos que tengan relación con la relación entre ambos.

Aquí podemos observar en el archivo NOTA la mención a los datos especialmente protegidos:


Fuente: Agencia Española de Protección de Datos

### 1.1.13 Finalidad del fichero y usos previstos

Se deberá describir de forma detallada la finalidad y usos previstos del fichero, así como seleccionar la tipificación de finalidad que mejor se corresponda con la descrita.
En primer lugar, rellenaremos la definición que puede ser del estilo siguiente:
"Fichero maestro para la gestión de los clientes de la sociedad".
Una vez se ha descrito la finalidad del fichero, será necesario que se indiquen, marcando cuáles son las finalidades para las que se utilizan los datos.
Se puede marcar más de una finalidad, pero se recomienda que se marquen única y exclusivamente las que sean necesarias y constituyan realmente el objeto de los ficheros. Asimismo, será necesario que las finalidades, a las cuales se indique que se aplican los datos, hayan sido informadas al afectado en el momento de recabar sus datos.

### 1.1.14 Procedencia y procedimiento de recogida de los datos

En este apartado se deberán indicar tres aspectos relacionados con la procedencia y la recogida de los datos:

a) Procedencia de los datos: aquí se ha de señalar quién nos ha facilitado los datos o de dónde se han obtenido. En el caso que se indiquen que los datos proceden de otras personas físicas distintas del afectado, será necesario comunicarle que se disponen de sus datos y las personas que los han facilitado.
b) Procedimiento de recogida: será necesario indicar como mínimo un procedimiento de recogida.
c) Soporte utilizado: se deberá indicar cual es el soporte mediante el cual se han obtenido los datos.
Podemos observar una pequeña imagen del archivo NOTA en el que se hace referencia a este apartado:


Fuente: Agencia Española de Protección de Datos

### 1.1.15 Cesiones o comunicaciones de datos

Se cumplimentará este apartado únicamente cuando se prevea realizar cesiones o comunicaciones de datos, es decir, cuando los datos se entreguen a una tercera persona o empresa para que los utilice. Deberá indicarse el supuesto legal en que se ampara el responsable para proceder a la comunicación de datos y la identificación, mediante el NIF /CIF y nombre o razón social, de los destinatarios de la cesión o comunicación.

No se ha de confundir la cesión o comunicación de datos con el tratamiento por cuenta de terceros. Por ejemplo, en el caso que entreguemos los datos de los trabajadores a una gestoría para que nos preparen las nóminas, no estaremos ante una cesión sino un tratamiento por cuenta de terceros.

En el caso de que entreguemos los datos a otra empresa para que pueda utilizarlos para realizar publicidad de sus productos y servicios, estaríamos ante una cesión o comunicación.

### 1.1.16 Transferencias internacionales

Se cumplimentará para el caso que se realice o esté previsto realizar un tratamiento de datos fuera del territorio español por ejemplo un intercambio de alumnos españoles hacia otro país

o al revés. Las transferencias internacionales de datos deben ampararse en los supuestos contemplados en la LORD, por lo que deberá marcarse el correspondiente supuesto legal que habilita la realización de transferencias internacionales. Si no fuese éste el caso, deberá solicitarse la preceptiva autorización del Director de la APD.

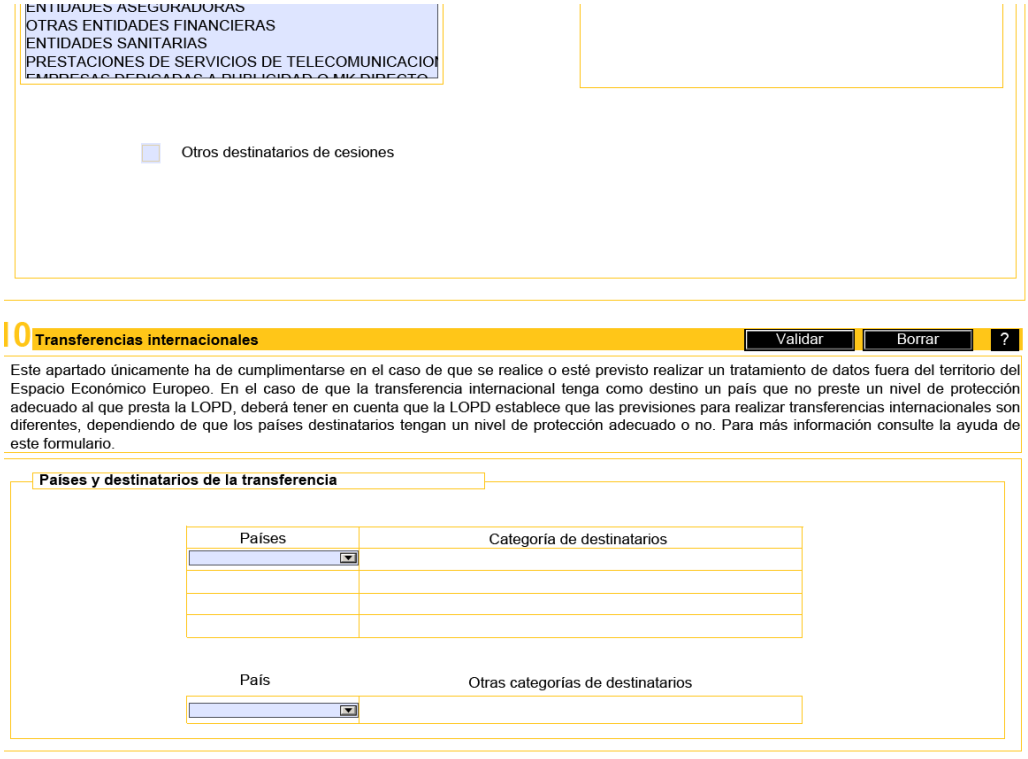
Por otra parte, un segundo subapartado se requiere indicar e identificar, mediante NIF / CIF y nombre o razón social, a los destinatarios de la transferencia internacional.

Los supuestos legales más habituales en que se amparan las transferencias internacionales de datos son:

a) Que la transferencia se realiza con destino a un país que proporcione un nivel de protección.

b) Que el afectado haya dado su consentimiento. Será necesario que en el momento de la recogida o posteriormente se recabe de forma expresa dicho consentimiento.

En la parte final del archivo que debemos de rellenar para completar la inscripción figura:




Fuente: Agencia Española de Protección de Datos

### 1.1.17 Inscripción.

De verificarse que la notificación remitida contiene toda la información preceptiva y cumple todas las exigencias legales, la APD acordará la inscripción del fichero en el Registro General de Protección de Datos. Éste notificará al responsable del fichero la inscripción.

En caso contrario, se requerirá al responsable indicado del fichero para que complete o subsane la información en el plazo de diez días. Transcurrido dicho plazo, se considerará que desiste de su petición y ésta quedará archivada.
En todo caso, si la APD no resuelve sobre la solicitud de inscripción en el plazo de un mes desde su presentación, se entenderá inscrito el fichero.
La inscripción del fichero en el Registro General de Protección de Datos únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la LOPD, y no con el resto de obligaciones previstas en la misma y sus disposiciones de desarrollo.

## 1.2 La intimidad, un derecho

La intimidad es un valor que se reconoce unánimemente en todo el mundo civilizado desde el Siglo XX. La intimidad ya fue recogida como uno de los derechos humanos en el artículo 12 de la Declaración Universal de Derechos Humanos (1944) donde se señala que: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”
En España, este derecho viene reconocido en el artículo 18 de la Constitución (1978) que señala lo siguiente:

> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

> 4. 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.

Observamos, por lo tanto, que la intimidad es uno de los derechos fundamentales que se recoge en el ordenamiento jurídico español, además de ser uno de los derechos humanos reconocidos internacionalmente. Deberemos tener muy en cuenta este derecho a la hora de implantar la Ley de Protección de datos sea cual sea el sector con el que trabajemos, máxime en el sector educativo donde podemos trabajar con menores de 14.

### 1.3 El concepto de "intimidad"

La pregunta es qué se entiende por "intimidad". Aunque caben muchas interpretaciones, podemos definir el derecho a la intimidad, hablando en general, como el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, de sus sentimientos, de sus emociones, de sus datos biográficos y personales y de su imagen. En términos técnico-jurídicos, puede hacerse una distinción bastante clara entre el derecho al honor, el derecho a la intimidad personal y el derecho a la propia imagen.

El derecho a la intimidad abarca muchas circunstancias de la vida personal.
Últimamente, con el desarrollo de la informática, la intimidad ha expandido el ámbito a que ella misma se refiere y se ha ido observando que las nuevas herramientas informáticas pueden suponer una intromisión en la vida privada de las personas. Por ello, el concepto de intimidad ha ido aproximando al de "privacidad". Es más que nada una cuestión de palabras. Lo que se denomina correctamente en castellano "intimidad" muchas veces la gente, empleando un anglicismo, lo llama "privacidad". El anglicismo trae causa de que los británicos denominan "private" a lo que no es "public", esto es, a aquellos ámbitos de la vida en los que los demás no tienen derecho a involucrarse, a lo íntimo. Así se han ido mezclando los conceptos de "intimidad" y "privacidad", de tal suerte que por privacidad se entiende no sólo a la facultad que una persona tiene para poder excluir a cualquier persona o ente del conocimiento de su vida personal sino que, además, se incluye la posibilidad de controlar que aspectos de esta vida personal, puedan ser conocidos por otras personas. La intimidad ha ido ampliando y mezclando su concepto, incluye la definición de privacidad y ofrece una doble faceta:

- Por un lado, será el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, sus sentimientos, sus emociones, sus datos biográficos y personales y su imagen.
- Por otro lado, además, será la facultad de determinar en qué medida esas dimensiones de la vida personal pueden ser legítimamente comunicadas o conocidas por otras personas.

El primer país que posee una legislación específica sobre protección de datos fue Suecia, en 1973. En Estados Unidos se dictó la "Privacy Act" (Ley de Privacidad) en 1974. La Constitución portuguesa de 1976 fue la primera Constitución en el mundo que limitó el uso de la informática para salvaguardar la intimidad: en su artículo 35 (1) estableció no solamente el derecho de acceso de los ciudadanos a los registros mecanográficos y la petición de su rectificación y actualización, sino que excluyó la posibilidad de usar la informática para tratamiento de datos referentes a las convicciones políticas, fe religiosa o vida privada excepto cuando se tratara un de proceso de datos no identificables para fines estadísticos.

En 1978, la Constitución española limitó el uso de la informática para preservar la intimidad de sus ciudadanos en el artículo 18.4 (2) (el referido a intimidad y que ya recogimos antes): "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."

**(1)CONSTITUCIÓN DE PORTUGAL DE 2 DE ABRIL DE 1976** Artículo 35.

Utilización de la informática

1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización.

2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.

**(2)CONSTITUCIÓN ESPAÑOLA Aprobada por Las Cortes en sesiones plenarias del Congreso de los Diputados y del Senado celebradas el 31 de octubre de 1978**

Artículo 18.

4. 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.

En 1992, tras un avance muy significativo de las nuevas tecnologías se dictó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal ("LORTAD"). Esta Ley ha sido sustituida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal ("LOPD"), dictada con el 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. Posteriormente, en el año 2007 se dictó el Real Decreto 1720/2007 que desarrolla y completa los flecos existentes en la LOPD 15/1999.

En la Unión Europea existen varias normas relativas a la protección de datos personales, entre las que podemos citar 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 (Directiva de Protección de Datos), y 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.

Se ha aprobado también la 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 (Directiva sobre la privacidad y las comunicaciones electrónicas, (DOCE 201/2002 de 31-07-2002).

## 2. Datos de "Carácter Personal"

Como dispone el Diccionario de la Real Academia de la Lengua Española dato es "Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho" y personal "Perteneciente o relativo a la persona" y como se indica en la primera definición del artículo 3 (1) de la Ley 15/1999 es cualquier información que hace identificadas o identificables a las personas o como se indica en el RD 1720/2007 es cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Se puede resumir como cualquier información que permita identificar o haga identificable a una persona identificable es un ato de carácter personal ya sea, por ejemplo, su nombre y

apellidos, su imagen o voz, y por tanto tendrá que ser tratada conforme a lo dispuesto en la normativa vigente sobre protección de datos.

Debido a la importancia que suponen para las empresas y para las personas se debe dotar de seguridad a estos datos personales. Las empresas deben inventariar estos datos y dotarlos de ciertas medidas de protección y seguridad, por una parte para cumplir con las disposiciones legales de las leyes actuales y por otra parte para asegurar que no se produzcan accesos a datos no consentidos que serían una ilegalidad y una falta de competitividad frente al resto de empresas del sector.

### 2.1 Tipología de los datos de carácter personal

Hay varios tipos de datos personales y la clasificación se puede llevar atendiendo a dos criterios:

- Según su importancia.
- Según su seguridad.

Según su importancia se clasifica a los datos personales en función de la relación que tienen esos datos personales con el derecho a la intimidad y en especial con los datos personales especialmente protegidos.
La relación de cuáles son esos datos especialmente protegidos está en los artículos 7 y 8 (2) de la LOPD y son los datos que tienen mayor relación con los aspectos más importantes del derecho a la intimidad como son los referidos a la ideología, religión, creencias, afiliación sindical, salud, vida sexual, origen racial o étnico y comisión de infracciones penales o administrativas.
Por otra parte, "datos personales" son todos los datos personales que no están especialmente protegidos.

**(1) Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal**. Artículo 3. Definiciones.
A los efectos de la presente Ley Orgánica se entenderá por:
a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

(2) **1) Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal**
Artículo 7. Datos especialmente protegidos.
1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
Artículo 8. Datos relativos a la salud. Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

El segundo criterio de clasificación de los datos personales (según su seguridad), está basado en las medidas de seguridad que se deben cumplir cuando se posean datos personales.
Estas medidas de seguridad se encuentran previstas en el artículo 9 de la LOPD y se desarrollan 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.

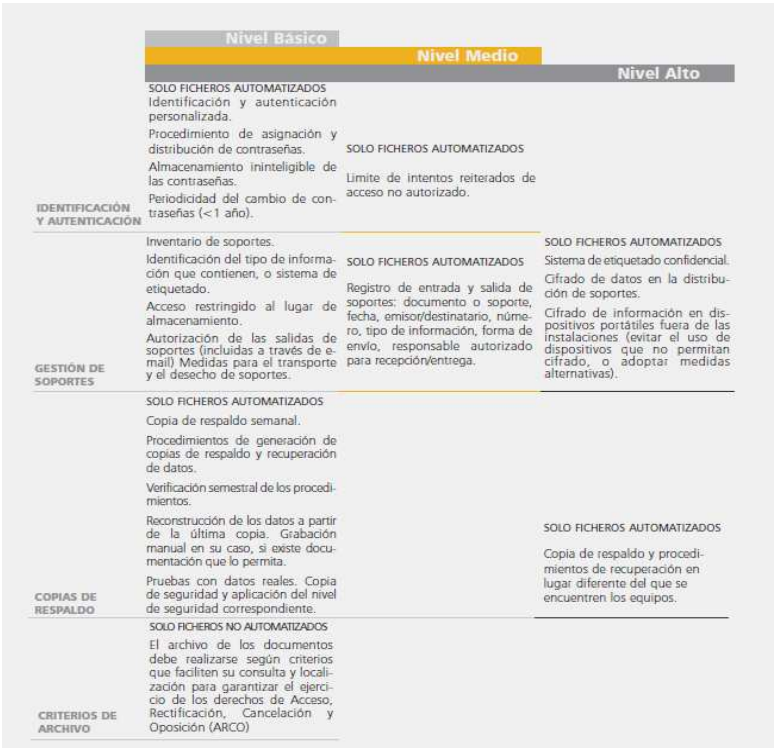
Tipos de datos en función de su seguridad:

- Datos de nivel básico: Todos los ficheros que contengan datos de carácter personal.
- Datos de nivel medio: Aquellos datos personales que permitan obtener una evaluación de la personalidad del individuo, datos personales relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y prestación de servicios de información sobre solvencia patrimonial y crédito.
- Datos de nivel alto: Aquellos datos personales relativos a la ideología, religión, creencias, origen racial, salud, vida sexual y datos recabados para fines policiales sin consentimiento del interesado y los datos que sean derivados de actos de violencia de género.

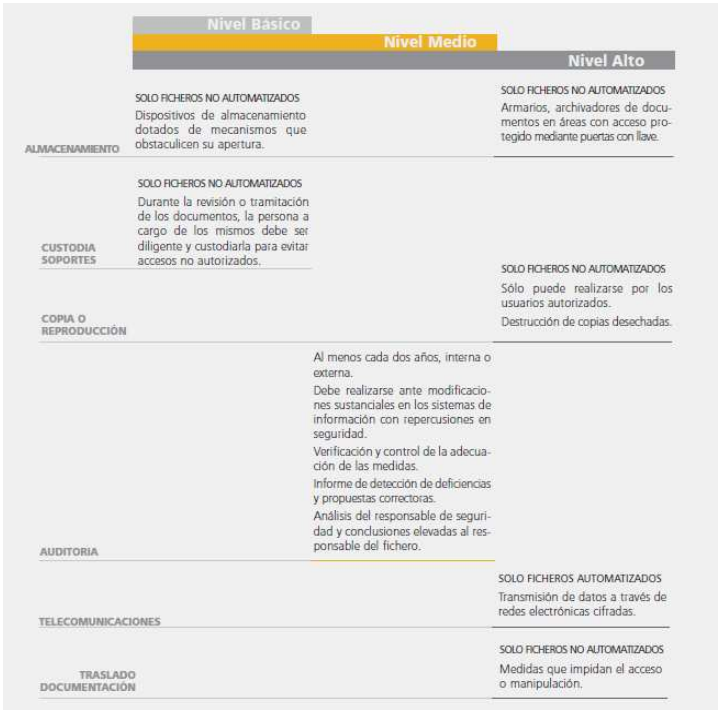
En este cuadro resumen podemos ver las medidas de seguridad en función del nivel de los datos tratados:

| | Nivel Básico | Nivel Medio | Nivel Alto |
|---|---|---|---|
| RESPONSABLE DE SEGURIDAD | | El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad).<br>El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento. | |
| PERSONAL | Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas.<br>Definición de las funciones de control y las autorizaciones delegadas por el responsable.<br>Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento. | | |
| INCIDENCIAS | Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras.<br>Procedimiento de notificación y gestión de las incidencias. | SOLO FICHEROS AUTOMATIZADOS<br>Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente.<br>Autorización del responsable del fichero para la recuperación de datos. | |
| CONTROL DE ACCESO | Relación actualizada de usuarios y accesos autorizados.<br>Control de accesos permitidos a cada usuario según las funciones asignadas.<br>Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.<br>Concesión de permisos de acceso sólo por personal autorizado.<br>Mismas condiciones para personal ajeno con acceso a los recursos de datos. | SOLO FICHEROS AUTOMATIZADOS<br>Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información. | SOLO FICHEROS AUTOMATIZADOS<br>Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado.<br>Revisión mensual del registro por el responsable de seguridad.<br>Conservación 2 años.<br>No es necesario este registro si el responsable del fichero es una persona física y es el único usuario.<br>SOLO FICHEROS NO AUTOMATIZADOS<br>Control de accesos autorizados.<br>Identificación accesos para documentos accesibles por múltiples usuarios. |

Fuente: Agencia Española de Protección de Datos



| | Nivel Básico | Nivel Medio | Nivel Alto |
|---|---|---|---|
| IDENTIFICACIÓN Y AUTENTICACIÓN | SOLO FICHEROS AUTOMATIZADOS<br>Identificación y autenticación personalizada.<br>Procedimiento de asignación y distribución de contraseñas.<br>Almacenamiento ininteligible de las contraseñas.<br>Periodicidad del cambio de contraseñas (<1 año). | SOLO FICHEROS AUTOMATIZADOS<br>Límite de intentos reiterados de acceso no autorizado. | |
| GESTIÓN DE SOPORTES | Inventario de soportes.<br>Identificación del tipo de información que contienen, o sistema de etiquetado.<br>Acceso restringido al lugar de almacenamiento.<br>Autorización de las salidas de soportes (incluidas a través de e-mail) Medidas para el transporte y el desecho de soportes. | SOLO FICHEROS AUTOMATIZADOS<br>Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega. | SOLO FICHEROS AUTOMATIZADOS<br>Sistema de etiquetado confidencial.<br>Cifrado de datos en la distribución de soportes.<br>Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas). |
| COPIAS DE RESPALDO | SOLO FICHEROS AUTOMATIZADOS<br>Copia de respaldo semanal.<br>Procedimientos de generación de copias de respaldo y recuperación de datos.<br>Verificación semestral de los procedimientos.<br>Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita.<br>Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente. | | SOLO FICHEROS AUTOMATIZADOS<br>Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos. |
| CRITERIOS DE ARCHIVO | SOLO FICHEROS NO AUTOMATIZADOS<br>El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) | | |



| | Nivel Básico | Nivel Medio | Nivel Alto |
|---|---|---|---|
| ALMACENAMIENTO | SOLO FICHEROS NO AUTOMATIZADOS<br>Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura. | | SOLO FICHEROS NO AUTOMATIZADOS<br>Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave. |
| CUSTODIA SOPORTES | SOLO FICHEROS NO AUTOMATIZADOS<br>Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados. | | |
| COPIA O REPRODUCCIÓN | | | SOLO FICHEROS NO AUTOMATIZADOS<br>Sólo puede realizarse por los usuarios autorizados.<br>Destrucción de copias desechadas. |
| AUDITORIA | | Al menos cada dos años, interna o externa.<br>Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad.<br>Verificación y control de la adecuación de las medidas.<br>Informe de detección de deficiencias y propuestas correctoras.<br>Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero. | |
| TELECOMUNICACIONES | | | SOLO FICHEROS AUTOMATIZADOS<br>Transmisión de datos a través de redes electrónicas cifradas. |
| TRASLADO DOCUMENTACIÓN | | | SOLO FICHEROS NO AUTOMATIZADOS<br>Medidas que impidan el acceso o manipulación. |

Fuente: Agencia Española de Protección de Datos

Es importante saber que los datos personales están altamente protegidos por la Ley. La utilización, no ya abusiva o fraudulenta, sino incluso negligente, de dichos datos es sancionable administrativamente con importantes multas y otro tipo de sanciones y está castigada como delito.

Para la protección del derecho a la intimidad en relación a los datos personales, en España, como en la mayoría de los estados del mundo occidental civilizado, es obligatorio el cumplimiento de una serie de requisitos legales que las entidades (públicas o privadas) que gestionan estos datos personales deben cumplir (sobre todo, medidas de seguridad para proteger dichos datos), y existen órganos administrativos especializados dedicados exclusivamente a velar por el cumplimiento de las normas protectoras al Derecho a la Intimidad en materia de datos personales. En España este órgano es la Agencia de Protección de Datos.

### 3. Derechos de las Personas en la Protección de Datos

La ley LOPD establece los derechos de las personas hacia sus datos personales como independientes de tal manera que puede entenderse que el ejercicio de ninguno de ellos sea condición para el ejercicio de otro. Asimismo, los derechos son personalísimos, es decir, que sólo pueden ser ejercitados por su titular o representante legal en el caso de menores de edad como ocurre en un centro educativo.

La atención al ejercicio de los derechos corresponde al responsable del fichero, que deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

La respuesta a la solicitud del ejercicio de los derechos de los afectados (1) tendrá que hacerse por un medio que permita acreditar el envío y la recepción.

El titular del fichero o tratamiento de datos de carácter personal está obligado a permitir y facilitar el ejercicio de los derechos de los interesados como reconoce al interesado la LOPD.

El ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero que deberá contener:

- Nombre y apellidos del interesado; fotocopia del DNI o pasaporte u otro documento identificativos o válido y en su caso de la persona que lo represente o instrumentos electrónicos equivalente así como el documento o instrumento electrónico acreditativo de tal representación.
- Petición en que se concreta la solicitud de derecho/s requeridos al titular.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de a petición que formula.

El responsable del fichero deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no los datos personales del afectado.

En el caso de que la solicitud no reúna los requisitos exigidos, el responsable del fichero deberá solicitar la subsanación de los mismos para posteriormente dar respuesta a la petición del interesado.

Las personas físicas pueden ejercer sus derechos ante quién posea datos personales de un interesado. Para realizar el ejercicio de sus derechos deberá presentarse copia del DNI, solicitud del derecho, dirección para responder al ejercicio del derecho, datos identificativos de la persona que quiere ejercer su derecho

**(1) Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de carácter personal** ***Artículo 14***. Derecho de consulta al Registro General de Protección de Datos. Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita. ***Artículo 15.*** Derecho de acceso. 1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes. ***Artículo 16***. Derecho de rectificación y cancelación. 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado. ***Artículo 17***. Procedimiento de oposición, acceso, rectificación o cancelación. 1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente. 2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

### 3.1 Derecho de impugnación de valoraciones (Art.13 LOPD) (1)

Este derecho faculta al interesado a impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
También serán impugnables aquellos actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad, pudiendo obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

Este derecho ofrece la posibilidad de limitar el uso de técnicas que faciliten una información o perfil del interesado que vayan más allá de los datos por él facilitados.

### 3.2 Derecho de Consulta al Registro General de Protección de Datos (Art. 14 LOPD)

Cualquier persona podrá acceder a recabar información del Registro General de Protección de Datos o de los Registros de Protección de Datos que las Agencias de Protección de Datos Autonómicas creen al afecto para cumplir con sus competencias en la materia. La información que se puede recabar es la relativa a conocer la existencia de tratamientos de datos de carácter personal, la finalidad de los mismos y la identidad del responsable del fichero. Dichos Registros se configuran legalmente como de consulta pública y gratuita, no existiendo limitación alguna para las consultas efectuadas por parte del interesado.

Es obligación del responsable del fichero la inscripción de los ficheros en el Registro General de Protección de Datos o en Registro de la Agencia de Protección de Datos Autonómica correspondiente cuando se trate de ficheros de su ámbito competencial.

**(1) Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de carácter personal** Artículo 13. Impugnación de valoraciones. 1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. 2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. 3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. 4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

### 3.3 Derecho de Acceso (Art. 15 LOPD)

El interesado podrá dirigirse al responsable del fichero con objeto de conocer que datos figuran en el mismo, cuál es el origen de los datos y las comunicaciones que se hubieran realizado o que se prevean realizar en el futuro. Este derecho será ejercitado de forma gratuita en intervalos no inferiores a doce meses salvo un interés legítimo acreditado.
En el ejerció del derecho el responsable tiene la obligación de responder en un plazo máximo de un mes a partir de la recepción del ejercicio de acceso por parte del interesado. En el caso de que no sea respondida su petición podrá el interesado interponer reclamación prevista en el artículo 8 de la LOPD.
Haya o no datos del afectado o interesado, el responsable del fichero tiene la obligación de responder a la petición formulada.
La información que se le suministre al interesado deberá ser legible e inteligible, sin utilizar ni claves ni códigos proporcionando todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como de la información disponible del origen de los datos, los cesionarios de los mismos y especificación de uso y finalidad de los mismos.

El responsable podrá denegar el derecho de acceso en el caso de que ya haya sido ejercitado el mismo derechos en los doce meses previos salvo que acredite un interés legítimo; podrá negarlo también en los supuestos que una ley o norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

En todo caso, el responsable informará al afectado a su derecho a recabar la tutela de la Agencia Española de Protección de datos o en su caso a las autoridades de control de las Comunidades Autónomas conforme a lo dispuesto al art. 18 de la LOPD.
Al ejercitar el ejercicio del derecho de acceso, el afectado podrá optar por recibir la información requerida a través de uno o varios de los siguientes sistemas de consulta:

- Visualización en pantalla
- Escrito, copia o fotocopia remitida por correo, certificado o no

- Telecopia
- Correo electrónico u otro sistema de comunicación electrónica
- Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o la naturaleza del tratamiento, ofrecido por el responsable.

### 3.4 Derecho de rectificación y cancelación (Art. 16 LOPD)

Se trata de derechos independientes que conceden al interesado para instar al responsable del fichero a rectificar aquellos datos que no plasmen o ajusten a las previsiones de la ley y en particular cuando no respondan a la realidad por ser inexactos o incompletos, o cancelarlos cuando hayan dejado de ser necesarios para la finalidad para que fueran recabados.

La solicitud de rectificación deberá incluir el dato o datos erróneos y la corrección que debe realizarse y deberá ser acompañada de la documentación justificativa de la rectificación requerida, a no ser que la misma dependa exclusivamente del consentimiento del interesado.

En el caso de querer cancelar un dato o datos, el afectado deberá indicar a que datos se refiere, aportando a l efecto la documentación que lo justifique.
Para el ejercicio de este derecho el responsable del fichero tendrá la obligación de responder en un plazo no superior a 10 días al interesado. En el caso de que no se responda de manera expresa a la solicitud, el interesado podrá interponer una reclamación como se recoge en el artículo 18 de la LOPD. Aun cuando el responsable no disponga de datos del interesado deberá igualmente responder a la petición.
En el caso de que se hubieran cedidos datos previamente a la rectificación o cancelación, el responsable del fichero deberá comunicarlo al cesionario para que en el mismo plazo desde la recepción proceda a la cancelación o rectificación de los mismos.
En este caso el cesionario no deberá comunicarlo al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la LOPD.
El derecho de rectificación debe hacerse efectivo en un plazo de 10 días naturales en el caso de ficheros de titularidad privada y de 10 días hábiles en el caso de ficheros de titularidad pública.
Cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso en las relaciones contractuales entre la persona o

entidad responsable del tratamiento y el interesado no podrá ejercerse la cancelación de los mismos.

Así mismo, podrá denegarse tanto el derecho de cancelación como rectificación en los supuestos en que así lo prevea una Ley o norma de derecho comunitario de aplicación directa o cuando éstas implican revelar a los interesados el tratamiento de los datos a los que se refiera el acceso.

Por último, el responsable del fichero puede denegar la rectificación o cancelación de los datos solicitada cuando considere que no procede.

### 3.5 Derecho de oposición (Art. 6.4 LOPD)

En los casos en los que no resulte el consentimiento expreso del interesado para el tratamiento de los datos y siempre que una Ley no disponga lo contrario, el interesado podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento quien resolverá sobre la solicitud en un plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido en plazo sin recibir el interesado respuesta expresa podrá éste interponer reclamación prevista en el art. 18 de la LOPD. En el caso de no disponer de datos del interesado deberá igualmente responder a la solicitud en tiempo y forma.

El responsable del tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud de oposición.

En el caso de ser reconocido el derecho al interesado se procederá a la exclusión de los datos relativos al mismo.

El titular de los datos deberá exponer los motivos en los que se fundamenta su solicitud de oposición.

### 3.6 Tutela de Derechos (Art. 18 LOPD)

En el caso de que sea denegados cualquiera de los derechos del interesado o representante legal en el caso de menores de edad, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos, o en su caso, al organismo competente de la Comunidad Autónoma

(Agencias de protección de Datos Autonómicas) que deberán asegurarse de la procedencia o improcedencia de la denegación de derechos.

El interesado presentará la reclamación como se indica en el artículo 117 del Real Decreto 1720/2007 expresando con claridad el contenido de la reclamación y los preceptos de la LOPD que se consideran vulnerados.

Una vez recibida la reclamación en la Agencia Española de protección de Datos o en el Organismos Autonómico competente, se dará traslado de la misma al responsable del fichero, para que en un plazo máximo de 15 días formule las alegaciones pertinentes. Una vez recibidas las alegaciones o transcurrido el plazo previsto, la Agencia de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá la reclamación realizada.

El plazo máximo para dictar y notificar resolución en el procedimiento de tutela será de seis meses, a contar desde la entrada de la reclamación formulada en la Agencia Española de Protección de Datos por parte del afectado. En caso de no ser dictada resolución en el plazo de seis meses, se entenderá que por silencio administrativo positivo se estima la reclamación formulada.

Si en la resolución de tutela se estimara la reclamación, el responsable del fichero tendrá 10 días para que haga efectivo el ejercicio de derecho requerido por el interesado dando cuenta por escrito a la Agencia Española de Protección de Datos de que ha ejercido el derecho reclamado en idéntico plazo.

### 3.7 Derecho a indemnización (Art. 19 LOPD)

Este derecho supone que los interesados que sufran algún daño o lesión en sus bienes o derechos debido al incumplimiento de las obligaciones del responsable del fichero tendrán derecho a una compensación que deberá acordarse por la vía juridiscional.

En función de si se tratan de fichero de titularidad pública o privada habrá que pedir responsabilidades de una manera u otra. En el caso de tratarse de ficheros de titularidad pública, la responsabilidad se exigirá conforme a la legislación que regula el régimen de responsabilidad de las Administraciones públicas.

En el caso de ficheros de titularidad privada deberá acudirse a los órganos de la jurisdicción ordinaria.

### 3.8 Excepciones al ejercicio de acceso, rectificación y cancelación

En algunos ficheros no podrán ejercitarse los derechos que tienen reconocidas las personas hacia sus datos personales como son:

- Ficheros de las Fuerzas y Cuerpos de Seguridad
- Ficheros de Hacienda Pública

En el caso de que no sean reconocidos los derechos al interesado por parte del responsable, deberá éste comunicarlo a Agencia Española de Protección de Datos para que ésta en su nombre tutele sus derechos.

## 4. Sistema educativo español-evolución

De manera resumida, recordar la amplitud de la legislación educativa. Así, la Ley Orgánica 8/1985, de 3 de julio, Reguladora del Derecho a la Educación (LODE), en el artículo 1 recogía que todos los españoles tienen derecho a una educación básica que les permita el desarrollo de su propia personalidad y la realización de una actividad útil a la sociedad, siendo ésta obligatoria y gratuita en el nivel de educación general básica. Esta ley prevé la creación de centros privados concertados y privados.

Posteriormente, la Ley Orgánica 1/1990, de 3 de octubre, de Ordenación General del Sistema Educativo (LOGSE), amplió a diez años la duración de la enseñanza básica y planteó, como objetivos básicos de las etapas de la misma, el proporcionar a los alumnos y alumnas una formación amplia, general y versátil que les permita incorporarse plenamente a la vida activa y acceder a una formación posterior, así como disfrutar de la cultura y del ocio. La obtención del Título de Graduado en Educación Secundaria Obligatoria (en lo sucesivo ESO) constituiría la garantía de que tales propósitos se habían alcanzado y, por ello, el derecho a la educación implicaba la obligación o compromiso del sistema educativo de arbitrar todos los medios posibles para que la obtención del título de graduado en ESO estuviera al alcance de todo el alumnado.

La LOGSE, en la consideración de la educación como servicio público, integró la enseñanza pública, la enseñanza privada y la enseñanza privada concertada, garantizando un período formativo común desde los seis hasta los dieciséis años, y transfirió a las Comunidades Autónomas, en la medida en que tienen plenamente asumidas sus competencias, la "tarea de completar el diseño y asegurar la puesta en marcha de la reforma".
En sus distintos artículos, la LOGSE, hasta la aprobación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación (en lo sucesivo LOE), establecía que el sistema educativo comprendía enseñanzas de régimen general y enseñanzas de régimen especial,

**Ley Orgánica 8/1985, de 3 de julio, Reguladora del Derecho a la Educación.** ***Artículo Primero.*** 1. Todos los españoles tienen derecho a una educación básica que les permita el desarrollo de su propia personalidad y la realización de una actividad útil a la sociedad. Esta educación será obligatoria y gratuita en el nivel de Educación General Básica y, en su caso, en la formación profesional de primer grado, así como en los demás niveles que la Ley establezca.
2. Todos, asimismo, tienen derecho a acceder a niveles superiores de educación, en función de sus aptitudes y vocación, sin que en ningún caso el ejercicio de este derecho esté sujeto a discriminaciones debidas a la capacidad económica, nivel social o lugar de residencia del alumno. 3. Los extranjeros residentes en España tendrán también derecho a recibir la educación a que se refieren los apartados uno y dos de este artículo.

estableciendo cómo se ordenará cada una de ellas, de la siguiente manera:
Enseñanzas de régimen general:

- Educación infantil
- Educación primaria
- Educación secundaria:
- Educación secundaria obligatoria (ESO)
- Formación profesional de grado medio
- Bachillerato
- Formación profesional de grado superior
- Educación universitaria.

Enseñanzas en régimen especial:

- Enseñanzas artísticas
- Enseñanzas de idiomas o deportivas.

La LOE señala, en su Exposición de Motivos, que "*se establece la estructura de las enseñanzas, recuperando la educación infantil como una etapa única y consolidando el resto de las enseñanzas actualmente existentes, por entender, que el sistema educativo ha encontrado en esa organización una base sólida para su desarrollo*".

La educación primaria y la educación secundaria obligatoria constituyen los diez años de enseñanza básica ya citada. La educación primaria comprende seis cursos académicos, desde los seis a los doce años de edad, y la ESO abarca cuatro cursos académicos, entre los doce y dieciséis años de edad. Los alumnos que, al terminar la ESO, han alcanzado los objetivos de la misma recibirán el Título de Graduado en ESO que faculta para acceder a las enseñanzas de educación secundaria post-obligatoria, es decir, al bachillerato, a la formación profesional específica de grado medio, a las enseñanzas profesionales de artes plásticas, y a las enseñanzas deportivas de grado medio. Los alumnos que cursan satisfactoriamente el bachillerato reciben el Título de Bachiller que les faculta para poder acceder a la educación superior (enseñanza universitaria, formación profesional de grado superior, enseñanzas profesionales de artes plásticas y diseño de grado superior, y enseñanzas deportivas de grado superior).

Para aquellos alumnos que no alcancen los objetivos de la ESO, existe otra opción que se concretan con el desarrollo de programas específicos de garantía social con el fin de proporcionarles una formación básica y profesional que les permita incorporarse a la vida laboral o proseguir sus estudios en las distintas enseñanzas reguladas en esta Ley y, especialmente, en la formación profesional específica de grado medio.

Los centros escolares que imparten las enseñanzas obligatorias no universitarias se concentran en cuatro tipos: colegios públicos, institutos de enseñanza secundaria, centros privados concertados y centros privados. Así los colegios e institutos públicos tienen como titular a la Consejería de Educación de la Comunidad Autónoma que, por tanto, es responsable de los tratamientos de datos personales que se realizan en los mismos.

Los colegios privados concertados tienen como titular una entidad privada pero, al tener un concierto en materia económica con la Comunidad Autónoma, una parte de los tratamientos que realizan con los datos personales de sus alumnos están condicionados por esta circunstancia por lo que parte de los ficheros son de titularidad pública y otros ficheros de titularidad privada.

## 5 Implantación de la Ley de Protección de Datos en Centros Educativos Públicos

Con este análisis se tratarán los aspectos que generalmente trascienden a los centros escolares público en relación a la LOPD.

### 5.1 Principios de información y consentimiento

Como se recoge en el artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) "*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa*".

El artículo 5.1 (1), relativo al derecho de información en la recogida de datos, establece que "*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*".

***Ley Orgánica 15/1999 de 13 de diciembre de Protección de datos personales 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 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.

Es por ello de vital importancia hacer cumplir la ley e informar del proceso que se está realizando cuando se está realizando el periodo de matrícula y de recogida de datos de carácter personal, aportando dentro del documento de matrícula clausulas informativas en las que se indique de manera clara e inequívoca la recogida de datos que se está realizando.
Por otro lado, se debe incluir cláusulas que hagan referencia a los derechos que tienen las personas al ser tratados sus datos personales como es el caso de los alumnos y de la familia de los mismos ya que no se incluye un texto que informe de la existencia de un fichero o tratamiento, de la finalidad y de los destinatarios de la información solicitada, así como de la identidad y dirección del responsable del tratamiento, ni del carácter obligatorio o voluntario de la respuesta a las preguntas que les plantean, ni de las consecuencias de la obtención de los datos o de la negativa a suministrarlos. Tampoco se informa de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Es más, dicha afirmación se hace extensiva a los formularios oficiales, que utilizan los centros y que están normalizados por las Consejerías de Educación, que no suelen llevar impreso ningún texto alusivo al artículo 5 de la LOPD y, en aquellos casos en los cuales se incorpora, éste no suele adecuarse a lo dispuesto en la normativa de protección de datos, incumpliendo de esta manera la Administración la LOPD. En Castilla y León el formulario si que cumple en principio la LOPD aunque sería conveniente que indicara la dirección física donde ejercitar los derechos de los interesados.

Debido a que en los formularios se suele omitir esta cláusula, los padres de los alumnos desconocen el destino de los datos personales que facilitan en los mismos, los tratamientos que va a realizar el centro escolar o la Consejería, la finalidad y los destinatarios de la información.

.

Remarcar la necesidad de recabar el consentimiento de los interesados, en este caso de los alumnos o representantes legales, como los padres o tutores legales en caso de separación o divorcio.

Respecto del derecho de información, las diferentes Consejerías de Educación, a través de los centros escolares públicos, recaban datos personales de los alumnos o de sus familias en las mismas situaciones; cuando una familia solicita plaza escolar, durante el proceso de

matriculación, para realizar gestiones diversas, como puede ser la tramitación de las becas convocadas, para gestionar la expedición de libros de escolaridad o de los títulos de graduado en ESO o bachillerato, así como para gestionar las pruebas de acceso a la universidad.

Los centros escolares, a su vez, recaban datos que pasarán a formar parte del expediente académico en soporte papel, y también necesitan conocer datos personales para prestar a los alumnos determinados servicios complementarios, tales como el servicio de comedor o las actividades extraescolares.

Los centros escolares comienzan a recoger datos personales en el momento en que los padres solicitan información para acceder a una plaza escolar en un centro público o, cuando éstos han sido admitidos, mediante distintos formularios que permiten formalizar la matrícula.

Estos formularios recaban datos personales del futuro alumno y de sus familias y son necesarios para que el centro escolar pueda prestar el servicio educativo solicitado.
Posteriormente, continúan recabando datos personales por distintos medios, procedentes de los padres, profesores, tutores y orientadores o incluso terceros, de tal forma que se completa el expediente académico.

Respecto del principio del consentimiento, los centros escolares, desde que reciben por primera vez a los padres o tutores solicitando plaza escolar, hasta que éste finaliza sus estudios en el centro o abandona el mismo para continuarlos en otro, necesitan realizar distintos tratamientos con los datos personales de las familias y de los alumnos.

Estos tratamientos se realizan utilizando soportes o ficheros informáticos, pero también manejan mucha información en soporte papel, tanto de documentación que ha aportado la familia, como listados y documentos que se extraen de los sistemas informáticos con distintas finalidades, o que elaboran los distintos profesionales que prestan sus servicios en el centro (orientadores, tutores o profesores).

Los centros escolares recaban y tratan gran cantidad de datos personales de las familias y de los alumnos y, como ya se ha especificado, al no facilitar la información del artículo 5 de la LOPD en los formularios utilizados para recoger los datos personales o facilitar una

información incompleta, no disponen del consentimiento regulado por la normativa de protección de datos para tratar los datos personales de sus alumnos y sus familias.

Los centros escolares realizan tratamientos que abarcan todo el ciclo escolar y que se encuentran regulados en la legislación vigente en materia educativa tanto nacional como autonómica. Estos tratamientos son necesarios para poder cubrir todo el servicio educativo, completar los ciclos educativos y emitir las titulaciones correspondientes. No obstante, no todos los tratamientos precisan contar con el consentimiento del alumno o de su familia, ya que algunos están habilitados por la normativa educativa que tiene rango de ley, por lo que, según el artículo 6.1 de la LOPD, no precisan del consentimiento citado.
A modo de ejemplo, los siguientes tratamientos no necesitarían consentimiento:

- Solicitud de plaza escolar,
- Libro de escolaridad,
- Gestión de solicitudes de becas
- Expedición de los títulos académicos.

Si necesitarán el consentimiento necesario para realizar otro tipo de tratamientos, tales como la publicación de fotos en los anuarios, o la entrega de datos de alumnos a los museos cuando se plantea su visita como una actividad extraescolar, en cuyo caso, es necesario contar con el consentimiento exigido por la LOPD.

Generalmente, la solicitud de datos personales por parte de los centros escolares y la entrega de los mismos por parte de las familias, suele ser una práctica tan habitual y generalizada que ambas partes creen que es un proceso natural que se encuentra amparado por la legislación educativa y todo ello debido al desconocimiento de la normativa por ambas partes. Es tal desconocimiento que en algunas ocasiones se solicita autorización de los padres o tutores para el tratamiento de datos cuando por imperativo legal no se necesario el consentimiento de los mismos.

### 5.2 Principio de calidad

El principio de calidad viene regulado en el artículo 4 de la LOPD y según se recoge en el mismo, "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". Además, estos datos no podrán utilizarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos, deben ser exactos y cancelados cuando dejen de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Atendiendo a lo anterior, en este apartado se han analizado los distintos momentos en que los centros escolares recaban datos personales, tanto de los alumnos como de sus familias, para analizar su tipología y valorar si pueden ser considerados adecuados, pertinentes y no excesivos en función del tratamiento posterior que va a realizarse con los mismos, tanto en los centros escolares como en la Consejería de Educación. También se analizan los datos personales que almacenan, la antigüedad y si disponen de procedimientos de cancelación o bloqueo de los mismos.
Los centros, a nivel general, y como ya se ha expuesto, recaban datos personales de los alumnos y de sus familias en distintos momentos. Dentro de ellos, se pueden destacar los que se desarrollan en el epígrafe siguiente.

### 5.3 Solicitud de plaza escolar

El proceso de admisión del alumnado en los centros docentes que impartan, sostenidas con fondos públicos, enseñanzas de Educación Infantil, Primaria, Secundaria Obligatoria y Bachillerato de la Comunidad de Castilla y León se encuentra regulado por el Decreto 17/2005, de 10 de febrero, modificado por el Decreto 8/2007, de 25 de enero, por el que se regula la admisión del alumnado en centros docentes sostenidos con fondos públicos de la Comunidad de Castilla y León; por la Orden EDU/184/2005, de 15 de febrero, modificada en varias ocasiones por la Orden EDU/133/2007, de 1 de febrero, la Orden EDU/2075/2008, de 27 de noviembre, y la Orden EDU/2380/ 2009, de 23 de diciembre, por la que se desarrolla el proceso de admisión del alumnado en los centros docentes que impartan, sostenidas con

Fondos Públicos, enseñanzas de Educación Infantil, Primaria, Secundaria Obligatoria y Bachillerato en la Comunidad de Castilla y León; y por último por la Resolución de 17 de febrero de 2005, de la Dirección General de Planificación y Ordenación Educativa, modificada mediante Resolución de 1 de febrero de 2007, sobre los procesos implicados en la admisión y matriculación de alumnos en centros docentes sostenidos con Fondos Públicos de Educación Infantil, Primaria, Secundaria Obligatoria y Bachillerato en la Comunidad de Castilla y León.

La gestión del proceso de admisión del alumnado se realizará a través de la denominada «aplicación informática de admisión». Los centros públicos y privados-concertados gestionarán los procesos de reserva de plaza y de libre elección de centro mediante la aplicación informática de admisión que se encuentra alojada en el «Portal de Educación» (http://www.educa.jcyl.es/), –> «Acceso privado», –> «Aplicaciones en línea» y –> «Admisión de alumnos».

El día 15 de junio de 2010 todos los centros destinatarios de alumnos procedentes de los procesos de reserva de plaza y de libre elección de centro, tendrán disponible en la aplicación informática de admisión, un fichero que contendrá los datos relativos a los alumnos admitidos en su centro, para la incorporación a sus aplicaciones informáticas de gestión.

Los centros comprobarán que todos los datos y documentación aportada se ajustan a la normativa aplicable, especialmente el domicilio familiar alegado, que deberá ajustarse en todo caso a lo dispuesto en el artículo 11 del Decreto 17/2005, de 10 de febrero y en el artículo 13.a) de la Orden EDU/184/2005, de 15 de febrero (1), de acuerdo con la redacción dada por la Orden EDU/2380/2009, de 23 de diciembre. Por cada solicitud se alegará únicamente un domicilio, pudiendo optar entre el domicilio familiar o el laboral.

Durante el proceso de solicitud de plaza escolar que a su vez es un proceso de recogida de información podemos reseñar como aspectos más importantes a tener en cuenta el proceso de cancelación de los datos en caso de no ser aceptado el alumnos en un centro escolar y el principio que recoge la LOPD en su artículo 4 que en relación a la calidad de los datos pidiendo datos adecuados, pertinentes y no excesivos en relación a la función por la que son recogidos que no es otra que la solicitud de plaza escolar.

Es una práctica común a todas las Comunidades Autónomas que los padres o tutores de los alumnos, para solicitar plaza en un centro público, cumplimenten un formulario normalizado por la respectiva Consejería de Educación de la Comunidad Autónoma, en el caso de Castilla y León podemos observar el la imagen la "Solicitud de admisión en centros docentes sostenidos con fondos públicos" y en el que se recaban datos personales del futuro alumno y de sus familias.

Los datos personales que se solicitan son los siguientes:

- Datos del alumno: nombre y apellidos, fecha y lugar de nacimiento, número de NIF, nacionalidad y número de NIE, en caso de extranjero.
- Datos de los padres o tutores: nombre y apellidos, número de NIF, nacionalidad y número de NIE en caso de que sean extranjeros.
- Grado de parentesco con el alumno.
- Estado civil de la persona solicitante de plaza escolar.
- Datos del domicilio familiar: dirección, números de teléfono.
- Datos del domicilio laboral: sólo se solicita en caso de que los solicitantes opten por ese domicilio a efectos de ser tenido en cuenta en el baremo.
- Datos académicos del curso actual.
- Datos del curso en el que estaba matriculado el curso anterior.
- Importe de la renta anual percibida por la unidad familiar.
- Si el padre/madre/tutor es trabajador de la Consejería de Educación o en pago delegado.
- Concurrencia de discapacidad en el alumno, padres o tutores y hermanos o hermanas, si tienen reconocido un grado igual o superior al 33%.
- Si los padres están desempleados o si tienen ingresos inferiores a 8000€.
- Concurrencia en el alumno de enfermedad crónica. En caso de que esa enfermedad afecte al sistema digestivo, endocrino o metabólico.

**(1) Orden EDU/184/2005, de 15 de febrero *Artículo 13*.** – Valoración y acreditación de los criterios de admisión .Los criterios de admisión se valorarán aplicando el baremo establecidos en el anexo I de la presente Orden. Su acreditación se realizará en los términos establecidos en el citado Decreto 17/05, y conforme a lo previsto en los apartados siguientes:
a) Proximidad del domicilio. Cuando se trate de alumnado escolarizado en régimen de internado, se considera r á , a efectos de escolarización en un centro determinad o , la residencia como su domicilio. En caso de que se desarrolle la actividad por cuenta propia, la proximidad del domicilio se acreditará mediante una certificación acreditativa del alta en la matrícula del Impuesto de Actividades Económicas y, en su caso fotocopia compulsada del pago de la cuota correspondiente al año en curso. En el supuesto de que no exista obligación legal de estar dado de alta en el Impuesto de Actividades Económicas, de conformidad con la normativa vigente, el domicilio laboral se acreditará mediante la presentación de una fotocopia compulsada de la correspondiente licencia de apertura expedida por el Ayuntamiento respectivo y una declaración responsable del interesado sobre la vigencia de la misma.

Podemos observar que se hace mención a los derechos de las personas al tratarse con datos personales aunque no se hace mención precisa de la dirección a la que deben de dirigirse en caso de querer ejercitar los derechos que les corresponden.

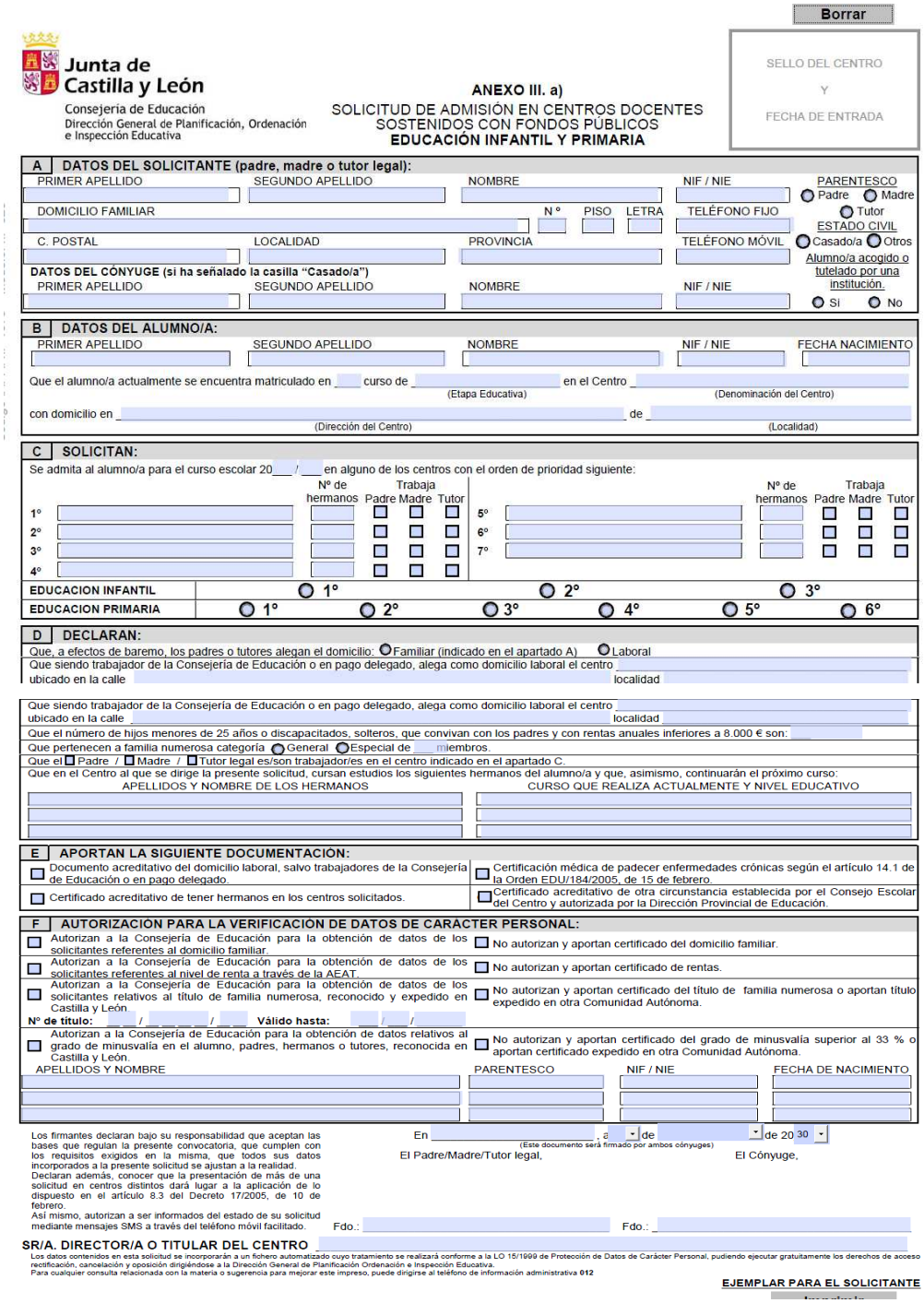
Tampoco se observa ninguna cláusula informativa en la que se haga mención de que es lo que se realizará en el caso de que al alumno no le sea otorgada una plaza escolar en los centros solicitados.

En la parte final de la solicitud se solicitan diferentes autorizaciones para poder solicitar la documentación necesaria para obtener la baremación pertinente o en caso de no autorización la entrega de la documentación en otro tipo de soporte para la pertinente comprobación de veracidad de datos y otorgar los puntos a los que se tiene derecho y que harán que sea más probable el otorgamiento de una plaza escolar en el centro o centros indicados. Además, hay un apartado en el que se indica que documentación se va aportar en la solicitud.

Se observa debajo la solicitud a cumplimentar en la Junta de Castilla y León en el proceso de admisión en Centros Docentes sostenidos con Fondos Públicos para el curso académico 2010/2011.

La documentación que se solicita para que acompañe a la solicitud de plaza escolar suele ser el certificado de empadronamiento en el que conste que el alumno vive con los padres o con alguno de ellos, certificado de la empresa donde trabajan sus padres o certificado que acredite la ubicación del trabajo si trabajan por cuenta propia, copia de la declaración de la renta familiar o declaración jurada de no tener ingresos o autorización para que la Consejería solicite esta información a la Agencia Estatal de Administración Tributaria, situación laboral de los padres y, en su caso, certificado de discapacidad o minusvalía del solicitante, ascendientes o hermanos en edad escolar, certificado de enfermedad crónica que afecte al sistema digestivo, endocrino o metabólico, certificado de familia numerosa, dictamen de los Equipos de Orientación Educativa Psicopedagógica sobre pertenencia a minoría étnica o inmigrante con déficit social o cultural, o sobre necesidades educativas especiales, acreditación de familia monoparental y expediente académico para solicitudes de plaza en los institutos de enseñanza secundaria. En algún caso, cuando el futuro alumno presenta un problema de salud (asma, diabetes, etc.) se solicita prescripción médica, o cuando los padres

tienen que acreditar que la guarda y custodia no es compartida debiendo aportar sentencia judicial en la que se indique quien es el que posee la custodia. Sería importante indicar también si existe alguna orden de alejamiento.



Borrar

Junta de Castilla y León
Consejería de Educación
Dirección General de Planificación, Ordenación e Inspección Educativa

SELLO DEL CENTRO
Y
FECHA DE ENTRADA

**ANEXO III. a)**
SOLICITUD DE ADMISIÓN EN CENTROS DOCENTES SOSTENIDOS CON FONDOS PÚBLICOS
**EDUCACIÓN INFANTIL Y PRIMARIA**

**A DATOS DEL SOLICITANTE (padre, madre o tutor legal):**

PRIMER APELLIDO | SEGUNDO APELLIDO | NOMBRE | NIF / NIE | PARENTESCO: Padre / Madre / Tutor
DOMICILIO FAMILIAR | Nº | PISO | LETRA | TELÉFONO FIJO | ESTADO CIVIL: Casado/a / Otros
C. POSTAL | LOCALIDAD | PROVINCIA | TELÉFONO MÓVIL | Alumno/a acogido o tutelado por una institución: Si / No

**DATOS DEL CÓNYUGE (si ha señalado la casilla "Casado/a")**
PRIMER APELLIDO | SEGUNDO APELLIDO | NOMBRE | NIF / NIE

**B DATOS DEL ALUMNO/A:**

PRIMER APELLIDO | SEGUNDO APELLIDO | NOMBRE | NIF / NIE | FECHA NACIMIENTO

Que el alumno/a actualmente se encuentra matriculado en ___ curso de _____ (Etapa Educativa) en el Centro _____ (Denominación del Centro)

con domicilio en _____ (Dirección del Centro) de _____ (Localidad)

**C SOLICITAN:**

Se admita al alumno/a para el curso escolar 20___ / ___ en alguno de los centros con el orden de prioridad siguiente:

| | | Nº de hermanos | Trabaja Padre | Trabaja Madre | Trabaja Tutor |
|---|---|---|---|---|---|
| 1º | | | ☐ | ☐ | ☐ |
| 2º | | | ☐ | ☐ | ☐ |
| 3º | | | ☐ | ☐ | ☐ |
| 4º | | | ☐ | ☐ | ☐ |
| 5º | | | ☐ | ☐ | ☐ |
| 6º | | | ☐ | ☐ | ☐ |
| 7º | | | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| EDUCACION INFANTIL | ○ 1º | ○ 2º | ○ 3º | | |
| EDUCACION PRIMARIA | ○ 1º | ○ 2º | ○ 3º | ○ 4º | ○ 5º | ○ 6º |

**D DECLARAN:**

Que, a efectos de baremo, los padres o tutores alegan el domicilio: ○ Familiar (indicado en el apartado A) ○ Laboral
Que siendo trabajador de la Consejería de Educación o en pago delegado, alega como domicilio laboral el centro _____ ubicado en la calle _____ localidad _____

Que siendo trabajador de la Consejería de Educación o en pago delegado, alega como domicilio laboral el centro _____ ubicado en la calle _____ localidad _____
Que el número de hijos menores de 25 años o discapacitados, solteros, que convivan con los padres y con rentas anuales inferiores a 8.000 € son: ___
Que pertenecen a familia numerosa categoría ○ General ○ Especial de ___ miembros.
Que el ☐ Padre / ☐ Madre / ☐ Tutor legal es/son trabajador/es en el centro indicado en el apartado C.
Que en el Centro al que se dirige la presente solicitud, cursan estudios los siguientes hermanos del alumno/a y que, asimismo, continuarán el próximo curso:

| APELLIDOS Y NOMBRE DE LOS HERMANOS | CURSO QUE REALIZA ACTUALMENTE Y NIVEL EDUCATIVO |
|---|---|
| | |
| | |
| | |

**E APORTAN LA SIGUIENTE DOCUMENTACIÓN:**

☐ Documento acreditativo del domicilio laboral, salvo trabajadores de la Consejería de Educación o en pago delegado.
☐ Certificado acreditativo de tener hermanos en los centros solicitados.
☐ Certificación médica de padecer enfermedades crónicas según el artículo 14.1 de la Orden EDU/184/2005, de 15 de febrero.
☐ Certificado acreditativo de otra circunstancia establecida por el Consejo Escolar del Centro y autorizada por la Dirección Provincial de Educación.

**F AUTORIZACIÓN PARA LA VERIFICACIÓN DE DATOS DE CARÁCTER PERSONAL:**

☐ Autorizan a la Consejería de Educación para la obtención de datos de los solicitantes referentes al domicilio familiar. ☐ No autorizan y aportan certificado del domicilio familiar.
☐ Autorizan a la Consejería de Educación para la obtención de datos de los solicitantes referentes al nivel de renta a través de la AEAT. ☐ No autorizan y aportan certificado de rentas.
☐ Autorizan a la Consejería de Educación para la obtención de datos de los solicitantes relativos al título de familia numerosa, reconocido y expedido en Castilla y León. ☐ No autorizan y aportan certificado del título de familia numerosa o aportan título expedido en otra Comunidad Autónoma.
**Nº de título:** ___ / _____ / ___ **Válido hasta:** ___ / ___ / ___
☐ Autorizan a la Consejería de Educación para la obtención de datos relativos al grado de minusvalía en el alumno, padres, hermanos o tutores, reconocida en Castilla y León. ☐ No autorizan y aportan certificado del grado de minusvalía superior al 33 % o aportan certificado expedido en otra Comunidad Autónoma.

| APELLIDOS Y NOMBRE | PARENTESCO | NIF / NIE | FECHA DE NACIMIENTO |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

Los firmantes declaran bajo su responsabilidad que aceptan las bases que regulan la presente convocatoria, que cumplen con los requisitos exigidos en la misma, que todos sus datos incorporados a la presente solicitud se ajustan a la realidad.
Declaran además, conocer que la presentación de más de una solicitud en centros distintos dará lugar a la aplicación de lo dispuesto en el artículo 8.3 del Decreto 17/2005, de 10 de febrero.
Así mismo, autorizan a ser informados del estado de su solicitud mediante mensajes SMS a través del teléfono móvil facilitado.

En _____, a ___ de _____ de 20 30
(Este documento será firmado por ambos cónyuges)
El Padre/Madre/Tutor legal, El Cónyuge,
Fdo.: _____ Fdo.: _____

**SR/A. DIRECTOR/A O TITULAR DEL CENTRO** _____

Los datos contenidos en esta solicitud se incorporarán a un fichero automatizado cuyo tratamiento se realizará conforme a la LO 15/1999 de Protección de Datos de Carácter Personal, pudiendo ejecutar gratuitamente los derechos de acceso rectificación, cancelación y oposición dirigiéndose a la Dirección General de Planificación Ordenación e Inspección Educativa.
Para cualquier consulta relacionada con la materia o sugerencia para mejorar este impreso, puede dirigirse al teléfono de información administrativa 012

**EJEMPLAR PARA EL SOLICITANTE**

Además en otras Comunidades Autónomas se recaba, en el proceso de admisión, otro tipo de documentación dentro del proceso de matriculación como la relativa a la opción religiosa, ruta escolar, copia de la cartilla de vacunación o, en su caso, certificado médico relativo a la salud del alumno.

En cuanto a la cancelación de datos, se debe distinguir entre los incluidos en los sistema de información automatizado utilizados por los centros escolares para baremar las solicitudes, y la destrucción de los formularios de solicitud de plaza y la documentación, en soporte papel, que se genera durante el proceso de admisión de alumnos.

En Castilla y León el sistema de admisión en el curso escolar 2010/2011 funciona como vemos en el gráfico inferior:


Fuente: Junta de Castilla y León (www.jcyl.es )

Generalmente los centros escolares utilizan una aplicación informática para baremar las solicitudes que, en algunos casos, es la misma que permite gestionar los datos personales de los alumnos y, en otros, es una aplicación específica. En Castilla y León una vez que se termina el proceso de admisión y el plazo de reclamaciones, la Administración proporciona a todos los centros (receptor de solicitudes y destino de los alumnos) tendrán disponibles en la aplicación los listados definitivos de adjudicación para su comprobación e impresión.

No obstante, se dan distintas situaciones ya que, en aquellos casos en los cuales el centro escolar admite a todos los solicitantes, los datos personales recabados se mantienen y, en principio, se consideran alumnos del centro. Sin embargo, cuando no se admite a todos los alumnos, algunos centros escolares nunca cancelan la información disponible de los alumnos no admitidos aunque en otros casos, la mantienen un año académico y, cuando se inicia el siguiente proceso de admisión, la eliminan.

Respecto de los formularios en soporte papel y la documentación anexa, se debe asegurar la eliminación de la documentación en el caso de que el alumno no haya sido admitido en un centro escolar pudiéndose añadir a la hoja de matrícula una cláusula informativa en la que se indique que se realizará con la documentación entregada si el alumno no es matriculado en el centro por parte de la Administración al tratarse de un proceso del que se hace cargo la Junta de Castilla y León.

Si el alumno ha sido admitido, la documentación se incluye en el expediente académico o, en algún caso, se excluye la declaración de la renta y el certificado de empadronamiento.

El proceso de admisión en los centros docentes públicos en la Comunidad
Autónoma de Castilla y León está regulado por el Decreto 8/2007 de 25 de enero que modifica al Decreto 17/2005 de 10 de febrero por el que se regula la admisión de alumnado a centros educativos financiados por fondos públicos de la Comunidad de Castilla y León. Donde se establecen los plazos de tramitación, y se recoge el formulario que deben utilizar los centros públicos y la documentación que deben aportar las familias junto al mismo. Esto significa que los datos solicitados en los formularios se consideran adecuados, pertinentes y no excesivos para la finalidad para la cual se recaban, que es baremar la solicitud atendiendo a los diversos conceptos recogidos en la normativa autonómica.

No obstante, en los casos en los que los centros escolares recaban otro tipo de documentación e información que no esté regulada en el citado proceso de admisión, ésta se considera excesiva para la finalidad para la que se está recabando como por ejemplo aficiones de los padres u otro tipo de informaciones que poco tienen que ver con el proceso educativo.

Los centros escolares no reciben instrucciones de la Consejería de Educación que les oriente sobre cuándo y cómo deben destruir la documentación relativa a las solicitudes de plaza escolar por lo que convendría que la Comunidad Autónoma dictase unas instrucciones precisas en relación al proceso de archivo y mantenimiento de datos referentes al proceso de admisión de alumnos, ya que los centros escolares desconocen qué funciones deben realizar en relación a este asunto.

### 5.4 Proceso de matriculación

La mayoría de las Comunidades Autónomas no elaboran una normativa específica a seguir por sus centros escolares cuando han de matricular a los alumnos que han obtenido plaza escolar. En el caso de Castilla y León los Centros Privados-Concertados y Públicos suelen usar modelos similares a la hoja de solicitud de plaza escolar, no en el formato pero si en la información que se pide a cada familia para cumplimentar y finalizar la matrícula.

Esto implica que cada centro escolar suela elaborar un formulario que es el que utiliza para matricular a sus alumnos, no existiendo uniformidad en los datos solicitados por ello sería adecuado que la Junta de Castilla y León homogeneizara un modelo únicos para todos los Centros Educativos financiados con Fondos Público como es el caso de los Colegios Públicos y los Colegios Privado-Concertados.

Es habitual, a casi todos los centros escolares, solicitar datos personales identificativos y académicos del alumno así como datos del sus padres (nombre y apellidos, DNI, teléfonos de contacto, estudios, profesión, empresa en la que trabajan y situación laboral) que como ya hemos indicado es similar a los datos requeridos en la solicitud de admisión o reserva de plaza escolar.

También es habitual solicitar alguna documentación adicional como pudieran ser certificados médicos, si el alumno precisa alguna atención especial, copia de la tarjeta sanitaria o de la cartilla de vacunación, fotocopia de los DNI de los padres, del libro de familia y, si los padres están separados, copia de la sentencia judicial en la que se especifica quién tiene asignada la custodia.

En esta Comunidad Autónoma no existe por el momento una legislación que regule la información que se ha de solicitar en la matriculación de los alumnos.
En la ORDEN EDU/1951/2007, de 29 de noviembre de Castilla y León en la disposición adicional primera se hace referencia a los datos personales del alumno y en concreto a el tratamiento de sus datos personales que se ajustará a los dispuesto en la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación y en la Ley 15/1999, de 13 de diciembre, de Protección de Datos Personales, por los que ciñéndonos a los artículos 4 y 5 de ésta última, los datos no serán excesivos, serán pertinentes y no excesivos para el fin para el que fueron recabados.

Además serán cancelados en el caso de que ya hubieran cumplido su fin, aspecto muy importante a tener en cuenta por ambas parte, es decir, tanto por la Administración, es este caso la Consejería de Educación como por parte del Centro Educativo que en su momento tuvo acceso a datos personales del alumno. En el caso de que el alumno haya estado escolarizado en un Centro tras dos años deberá cancelar y eliminar esos Datos Personales y no almacenarlos de manera indefinible como ocurre en muchas situaciones.

Como ya hemos indicado anteriormente y teniendo en cuenta la LOPD se deberá de informar antes de una recogida de datos, cosa que no suele ocurrir, ni a donde se dirigen los datos ni de los derechos que el interesado o este caso los padres/tutores por tratarse de menores de 14 años tienen al ser realizado un tratamiento de datos personales.

En el citado proceso, se han observado que, aunque no ha elaborado una legislación específica que regule la información que han de solicitar los centros escolares para matricular a sus alumnos, ha elaborado el formulario que deben emplear y en el cual se amplían los datos personales recabados durante el proceso de solicitud de plaza.

En Castilla y León se entrega lista de alumnado admitido a cada Centro pero no de modelos de matrícula unificado. También se da el caso de centros escolares que unifican el procedimiento de admisión junto con el de matriculación o de alguna Comunidad Autónoma en la que todos sus centros escolares utilizan el mismo formulario de matriculación que extraen de la aplicación informática que utilizan.

En los Centros Privados-Concertados tienen un programa informático que requieren los siguientes datos a rellenar por el Centro Escolar que puede tener relación bastante similar con los datos que contenga la matrícula:

Formato del fichero de exportación de datos de alumnos admitidos para centros concertados — Servicio de Informática

| Campos de información | | | |
|---|---|---|---|
| **Orden** | **Descripción** | **long. max.** | **Comentarios** |
| 1 | Año del proceso de admisión en curso | 4 | |
| 2 | Contador. | 4 | Comenzará con el valor 0001 y se incrementará en una unidad por cada registro. |
| 3 | Proceso de admisión | 1 | R → Reserva de plaza<br>L → Libre elección |
| 4 | Primer apellido del alumno | 25 | |
| 5 | Segundo apellido del alumno | 25 | |
| 6 | Nombre del alumno | 25 | |
| 7 | Sexo del alumno | 1 | V → Varón<br>M → Mujer |
| 8 | NIF del alumno | 9 | |
| 9 | Fecha de nacimiento del alumno | 10 | El formato será *dd/mm/yyyy* |
| 10 | Dirección | 77 | Contiene el tipo de vía, nombre, número, piso y letra |
| 11 | Nombre de la Localidad | 45 | |
| 12 | Nombre de la Provincia | 25 | |
| 13 | Teléfono | 9 | |
| 14 | Código postal | 5 | |
| 15 | Primer apellido del representante 1 | 25 | |
| 16 | Segundo apellido del representante 1 | 25 | |
| 17 | Nombre del representante 1 | 25 | |
| 18 | NIF del representante 1 | 9 | |
| 19 | Primer apellido del representante 2 | 25 | |
| 20 | Segundo apellido del representante 2 | 25 | |
| 21 | Nombre del representante 2 | 25 | |
| 22 | NIF del representante 2 | 9 | |
| 23 | Enseñanza adjudicada | 3 | EI → Educación Infantil<br>PRI → Primaria<br>ESO → Secundaria<br>BAC → Bachillerato |
| 24 | Familia adjudicada | 4 | En solicitudes de Educación Infantil la familia será EI.<br>En solicitudes de Primaria la familia será PRI.<br>En solicitudes de Bachillerato se codificarán las familias de la siguiente manera:<br>ARE → Artes Plásticas, Imagen y Diseño<br>ARP → Artes escénicas, Música y Danza<br>CIT → Ciencias y Tecnología<br>HCS → Humanidades y Ciencias sociales |
| 25 | Curso adjudicado | 1 | |

Fuente: Junta de Castilla y León

En algún centro escolar, el tutor del alumno admitido mantiene una entrevista personal con los padres o tutores y cumplimenta un formulario en el que incluye datos personales del alumno, datos sobre su evolución (salud principalmente), antecedentes de escolarización, alimentación, sueño, conducta, religión, composición familiar y antecedentes familiares.

Cuando se trata de alumnos que proceden de otros centros, los colegios o institutos suelen solicitar del centro de procedencia del alumno, el libro de escolaridad, el expediente académico, informes psicopedagógicos y el resto de la documentación si se trata de un alumno con necesidades educativas especiales.

En general, los datos recabados en los formularios de matriculación se consideran adecuados, pertinentes y no excesivos para la finalidad para la cual se recaban.

Sin embargo, sí podrían considerarse excesivos los datos relativos a DNI, estudios, profesión y situación laboral, tanto de la madre como del padre, o algunos datos que solicitan algunos centros escolares debería revisarse para no incumplir el artículo 4 de la LOPD (sueño, conducta, problemas que presentan los hermanos, etc.), ya que no está muy justificada la finalidad para la cual se están recabando que teóricamente es la enseñanza y matriculación de un alumno.

Los datos personales incluidos en los formularios de matriculación se incluyen en los sistemas informáticos no existiendo, con carácter general, una política de cancelación de los mismos, por lo que los datos son conservados indefinidamente incluso cuando el alumno abandona el centro escolar para trasladarse a otro o cuando ha finalizado completamente sus estudios.

En aquellos centros escolares que utilizan sistemas informáticos centralizados en la Consejería de Educación de la Consejería de Educación, en unos casos se desconoce la política de cancelación y en otros, cuando el alumno finaliza sus estudios, el sistema únicamente permite consultar los datos académicos del alumno y el motivo de baja en el sistema. Por ello, se debería formar más a los centros o responsables de éstos para que cancelen los datos personales cuando corresponde que en este caso son a los dos años de finalizar la relación de alumno-centro.

Los formularios en soporte papel y la documentación que se adjunta se incorporan en una carpeta que, posteriormente, constituirá el "expediente académico" del alumno que se suma a los datos informáticos que tiene el Centro en posesión y que también deben ser cancelados y no dejarlos almacenados de manera indefinida.

Sería importante informar a los Centros mediante una Orden o Ley de la obligación de Cancelación de datos y documentos que los contengan como el expediente académico.

### 5.5 Gestión de becas de estudios

Las familias de los alumnos escolarizados en centros públicos pueden solicitar becas y ayudas convocadas por el Ministerio de Educación. En este caso, los centros escolares

únicamente recaban la documentación, relacionen las solicitudes recibidas y las remiten a la Consejería de Educación de su Comunidad Autónoma.

Además, la Comunidad Autónoma de Castilla y León, a través de su Consejería de Educación, convoca becas y ayudas de distinto tipo que se publican en el BOCYL. En este caso, la Consejería anualmente publica la convocatoria correspondiente donde se indica el procedimiento a seguir por los centros escolares y, además, se publica el formulario que deben emplear las familias de los alumnos y la documentación a incluir.

En todos los casos, los datos personales que se solicitan se refieren al alumno, a sus padres o tutores, otros miembros de la unidad familiar, y a la situación económica familiar.

Finalmente, la Consejería de Educación envía a los centros un listado con las becas concedidas que los centros escolares publican en sus tablones de anuncios por lo que es la Administración Autonómica la que realiza el tratamiento de los datos personales tanto en los centros públicos como privados.

Los datos y documentación que se recaba mediante los correspondientes formularios están regulados por Órdenes y Resoluciones que se actualizan anualmente, se consideran adecuados, pertinentes y no excesivos.

Por otra parte**,** los centros escolares elaboran listados que remiten a la Consejería de Educación a efectos de control de entrega de la documentación en la misma.
Los centros escolares suelen conservar los listados de becas concedidas por periodos indefinidos, y, en algunas ocasiones, los destruyen una vez que ha finalizado el plazo de publicación, por estas razones se debe indicar por parte de la Administración el tiempo que debe estar expuesta una lista y que hacer con la misma una vez haya realizado el cometido para el que fue destinado. Los centros escolares, generalmente no conocen cuál debe ser su papel, tanto a la hora de servir para remitir datos de los solicitantes como en el momento de exponer la relación de los becados en el tablón de anuncios, únicamente se fijan en la información que es enviada por parte de la Consejería de Educación a los Centros Escolares

en la que se dan instrucciones de informar en tablón de anuncios pero no se hace mención a la LOPD.

El desconocimiento por parte de de los Centros suele ser grande aunque si que podemos indicar que en Castilla y León se pone a disposición de los Centros Educativos tanto en el periodo de matrícula como de admisión un teléfono para resolver las dudas suscitadas durante el proceso de admisión y matriculación pudiendo también resolver dudas relacionadas con el tratamiento de los datos personales.

Por ello, resultaría conveniente que los Centros Escolares pidieran información y órdenes por escrito por el organismo correspondiente y así ser informados de las funciones que les corresponden en relación al proceso de recogida de datos durante el proceso de convocatoria de becas y evitar problemas derivados del incumplimiento de la LOPD.

### 5.6 Gestión del expediente académico

El expediente académico suele ser un fichero en soporte papel que se inicia cuando un alumno se matricula en el centro escolar. Consta de una carpeta que identifica a cada alumno y contiene la documentación generada en los procesos de solicitud de plaza y de matriculación.

Posteriormente, se completa, en algunos casos, con la documentación que aporta el centro de donde procede el alumno, informes de tutoría y las calificaciones obtenidas por el alumno en los distintos cursos académicos. El centro escolar añade al expediente los distintos informes de evaluación que va elaborando el tutor por cada curso académico, informes de tutoría y todos aquellos informes relevantes que se elaboran durante el ciclo escolar entre los que se incluyen las sanciones y amonestaciones que puedan realizarse al alumno. Incluso en algunos casos, se incluyen sentencias judiciales de padres separados donde consta la custodia del alumno.

Es importante destacar que el expediente académico de un alumno con necesidades educativas especiales puede contener también, certificado del grado de minusvalía, copia de su historia clínica y el dictamen de escolarización, además de los informes psicopedagógicos

elaborados por los equipos de orientación que contienen diagnósticos de minusvalías físicas, psíquicas o sensoriales. También se incluyen los dictámenes que elaboran los equipos de orientación una vez han sido devueltos por la Consejería de Educación.

Suele ser también bastante habitual que los departamentos de orientación tengan sus propios expedientes compuestos por toda aquella información recabada por el orientador, tanto de los padres como del centro escolar, las pruebas de evaluación utilizadas y los informes elaborados.

Respecto a la cancelación de datos se observa que en los centros escolares habitualmente se almacenan todos los expedientes académicos de forma indefinida. Entre la documentación antigua que custodian algunos centros escolares en los expedientes académicos se puede citar: la ficha personal con datos personales, familiares, médicos y psicológicos, ficha familiar con datos de la familia, ficha de matrícula con copia del libro de familia, datos psicológicos, etc. También suele ser una práctica habitual archivar copias de aquellos expedientes cuyos alumnos han cambiado de centro escolar y el original se remite al nuevo centro.

Por otra parte, los centros escolares utilizan sus sistemas informáticos para gestionar una parte del contenido del expediente académico, así suelen añadir a los datos recabados durante la solicitud de plaza y matriculación, las notas escolares, incidentes disciplinarios, tipificación de la falta asociada a un incidente, etc. Toda esta información, es práctica habitual mantenerla de forma indefinida no habiéndose detectado caso alguno en el que tengan definidos procedimientos de cancelación.

Finalmente, añadir que los departamentos de orientación, en algunos casos eliminan sus expedientes pero, en otros, los incorporan a los expedientes académicos del alumno. Se desconoce, sin embargo, cuál ha de ser el procedimiento de cancelación de esta información.

Los centros escolares incluyen en el expediente académico documentos que son necesarios para la gestión académica y administrativa. Se debe prestar atención a este aspecto para no incluir ni pedir información que no sea necesaria o que no esté requerida legalmente ya que estaremos violando el artículo 4 de la LOPD.

Por otra parte, es necesario hacer hincapié a los centros escolares de que incluyan la documentación recogida durante el proceso de solicitud de plaza debido a que esa información puede ser requerida y en ese caso no podríamos ejercer el derecho de acceso, rectificación, cancelación u oposición por no tener la documentación necesaria.

Se debe establecer y comprobar los tiempos legales de permanencia de un expediente de un alumno tanto en el sistema informático como el papel, así como los informes del servicio pedagógico para evitar un cúmulo innecesario de documentación que únicamente puede traer problemas si los datos que contienen los documentos salen a la luz y estemos violando así el deber de secreto y la intimidad de las personas.

Es necesario resaltar que resulta innegable la necesidad de que exista un expediente académico del alumno, en el que se recoja la gestión académica y administrativa de cada uno aunque legalmente se desconoce cuál ha de ser su contenido exacto en la Junta de Castilla y León, y, por ello, en algunos casos, se incluyen datos especialmente protegidos o datos referentes al proceso de solicitud de plaza. Por tanto, convendría definir el concepto, naturaleza y contenido del expediente académico, así como los procesos de archivo y, en su caso, eliminación del mismo ni los plazos legales en los que el centro escolar deba ser responsable del contenido y custodia del mismo.

### 5.7 Otros formularios de recogida de datos

Todos los centros escolares, además de los formularios citados anteriormente, suelen elaborar otros de distinta índole que les permite gestionar otros servicios asociados a su labor educativa (servicio de transporte, comedor o guardería, actividades extraescolares, pruebas de acceso a la universidad, solicitud del título correspondiente, o adherirse a la Asociación de Madres y Padres), entre otros).

En este caso estas empresas deben solicitar una autorización expresa de utilización de datos para que el colegio pueda realizar esa cesión de datos y en el caso de que se haga en horas extraescolares se deberá comenzar un nuevo proceso de recogida de datos e información

previa al interesado, informando de la finalidad de los datos recabados y la forma en que el afectado puede ejecutar sus derechos, es decir, indicando la dirección física donde ejercitar sus derechos y el responsable del tratamiento. El centro escolar desconoce qué tratamiento le da la empresa a los formularios, ya no se hace responsable el centro escolar de lo que pudiera ocurrir con los datos personales de los clientes.

En el caso de que se den datos a otro tipo de empresas externas al centro, los interesados deberán dirigirse al titular o responsable del tratamiento de datos para reclamar sus derechos.

### 5.8 Datos especialmente protegidos

Y es que es una realidad el que los centros escolares conocen datos de salud de los alumnos o de sus familiares desde el momento en el que la familia cumplimenta el formulario de solicitud de plaza para un centro escolar público. En estos formularios deben especificar y acreditar documentalmente, en su caso, la minusvalía o discapacidad, la enfermedad crónica que afecte al sistema digestivo, endocrino o metabólico del alumno que exija un control alimentario, las necesidades educativas especiales o si pertenece a una minoría étnica o inmigrante con déficit social o cultural. Toda esta información es necesaria a efectos de obtener la puntuación que permitirá admitir o no al alumno en el centro escolar solicitado y, en algunos casos, cuando el alumno es diagnosticado con necesidades educativas especiales, para asignarle a aquel centro escolar que mejor se adapte a sus necesidades.

Merece destacar, por su especial importancia, el tratamiento de datos psicológicos que se llevan a cabo tanto en los centros escolares que disponen de un servicio de orientación como en los Servicios de Orientación Educativa de la Consejería de Educación de las Comunidades Autónomas. Esta diferenciación está recogida en la legislación vigente en materia educativa donde se encuentran perfectamente delimitados dos tipos de servicios:

"Equipos Especializados de Orientación Educativa y Psicopedagógica", que atienden a los centros docentes y que están formados por distintos profesionales especialistas (psicólogos, pedagogos y trabajadores sociales además de maestros especialistas en audición y lenguaje), dependiendo de las Direcciones Provinciales de Consejería de Educación de la correspondiente Comunidad Autónoma, y que prestan servicio de asesoramiento y apoyo al

sistema escolar en sus diferentes niveles, especialmente en los colegios públicos que son los que carecen de estos servicios en su plantilla docente.

En el artículo 7 de la LOPD se define como datos especialmente protegidos los relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual. Dicho artículo recoge en sus apartados 1, 2, y 3 lo siguiente:

> "*1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.*
> *Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo."*
> *"2. 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..."*
> *"3. 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*".

Legalmente se ha establecido que, con carácter previo a la incorporación de los alumnos a cualquiera de los programas citados (Garantía Social, Diversificación Curricular o Educación Compensatoria), el orientador debe elaborar un "informe de incorporación", que debe remitirse a la Inspección de Educación de la Consejería que es la que autoriza la incorporación de los alumnos a los programas a través de las correspondientes Comisiones de Escolarización.

Esto significa que se pide autorización expresa para el tratamiento de los datos personales y en este caso de datos especialmente protegidos de alumnos para que los equipos psicopedagógicos puedan tratar a los alumnos que por necesidades diversas los requieren.

También solicitan información sobre el estado de salud del alumno, durante el desarrollo del curso académico, en aquellos casos en que no puede participar en las actividades deportivas programadas o de otra índole (como una excursión) en el curso escolar, no puede tomar determinado tipo de alimentos, si va a utilizar el servicio de comedor o si tiene algún tipo de enfermedad que obligue al centro a tener alguna atención especial con él como puede ser el caso de diabetes o alergias. También solicitan informes médicos (audiometría, oftalmológicos, etc.) cuando se trata de escolarizar alumnos que presentan un problema de salud (niños sordos, minusválidos, etc.).

Cuando se produce algún problema relacionado con la salud, los centros escolares suelen llamar a los padres e informarles de lo acaecido, o bien llevar al niño al centro de salud más cercano perteneciente a la Consejería de Salud de la Comunidad Autónoma en el caso de que no respondan los padres/tutores.

En casi todos los colegios, son los profesores, los tutores o los padres los que detectan algún tipo de problema en el alumno, que se pone en conocimiento de los orientadores del Equipo Psicopedagógico de la Consejería de Educación, a través de un documento que incluye información general del alumno y problema detectado.
El orientador es el que valora la situación a través de diferentes pruebas y elabora informes psicopedagógicos, de intervención o dictámenes que serán los que orienten sobre las necesidades del alumno en cuestión. En la mayoría de las ocasiones, el orientador convoca a la familia a una entrevista en la que solicita autorización para valorar al alumno y tomar decisiones para actuar sobre el problema detectado.

En aquellos casos en los que el centro escolar detecta que un alumno puede tener necesidades educativas especiales, el orientador realiza las pruebas de evaluación, pertinentes y necesarias, para poder elaborar un "informe de intervención". En este caso, el orientador cita a los padres para que firmen la propuesta de inclusión del alumno en un programa que permita atender las necesidades de su hijo y poder elaborar el dictamen correspondiente, que se remite al departamento correspondiente de la Consejería de Educación de la Comunidad Autónoma, que es quien debe emitir la resolución que considere oportuna para incluirle en el programa con necesidades educativas especiales que mejor se adapte a su problemática. Es

habitual que estos orientadores elaboren "informes de compensación", relativos a alumnos que presentan en el colegio un cierto retraso escolar debido a circunstancias desfavorables.
En estos informes hay muchos datos especialmente protegidos del interesado y que se pondrán en conocimiento tanto del orientador como del personal docente que trabaja con él para solucionar en la medida de lo posible el problema detectado y tener lo más integrado posible al alumno.

También se realizan pruebas de evaluación colectivas a los alumnos en distintos cursos académicos como ocurre en la actualidad en 4º de Primaria y en Segundo de la ESO en la que se evalúa el grado de conocimiento de los alumnos en las asignaturas instrumentales como son Matemáticas y Lengua que permiten determinar el perfil individual de aptitudes diferenciales y general o determinar el coeficiente de inteligencia del alumno, su potencial de aprendizaje o determinar el perfil de autoestima del alumno.

Es necesario solicitar consentimiento a los padres para realizar este tipo de pruebas por entender que se realizan como consecuencia de la necesidad de dar cumplimiento al derecho que tienen los alumnos de recibir la pertinente orientación escolar, personal, familiar y social que reconoce la legislación en materia de derechos de los alumnos.
También se da el caso en que el equipo de orientación, dentro de un programa de detección de precocidad en los alumnos, realiza evaluaciones de alumnos al objeto incorporarles en un programa tutelado por la Consejería de Educación de la correspondiente
Comunidad Autónoma y, además, facilitar a las familias pautas de actuación para con sus hijos.

Finalmente reiterar la necesidad de una autorización expresa de los padres o tutor para poder tratar datos especialmente protegidos a los cuales se deberá prestar especial atención a las medidas de seguridad correspondientes.

### 5.9 Medidas de seguridad

En el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), se establece en su punto 1 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 están expuestos, ya provengan de la acción humana o del medio físico o natural*".

El Reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre en el Título VIII de este reglamento desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

La mayoría de los centros escolares públicos de Castilla y León utilizan los programas informáticos que distribuye la Consejería de Educación para la gestión de los expedientes y las notas.
Los datos personales gestionados por estos programas se pueden encontrar información relativa a las necesidades educativas especiales de los alumnos, adaptaciones curriculares, control de absentismo escolar o expedientes disciplinarios.

Además, algunos centros escolares utilizan otras aplicaciones informáticas, también distribuidas por la Consejería de Educación de la Comunidad, que les permite gestionar sus fondos bibliográficos y realizar el control de préstamos o solicitar los títulos académicos.

Por otra parte, algunos centros escolares han implantado un sistema informático que permite dotar a los profesores de un dispositivo electrónico, en el que se han introducido los datos personales de sus alumnos, y que permite introducir en el sistema, en tiempo real, todas las incidencias académicas y de comportamiento del alumno aunque suele ser ya en la ESO.

Otros centros escolares han diseñado aplicaciones propias que les permiten, por ejemplo, gestionar las becas que solicitan los alumnos o facturar el servicio de comedor u otros servicios.

Así mismo, es la Consejería de Educación la que actualiza y pone al día los sistemas informáticos.

El conjunto de ficheros automatizados de los centros escolares se encuentran almacenados en una misma base de datos, ubicada en la Consejería de Educación de la Comunidad Autónoma, y sólo los usuarios autorizados de cada centro escolar podrán acceder a los datos personales de sus alumnos mediante una conexión vía Internet.

Con carácter general, estos sistemas permitirán gestionar información relativa a las solicitudes de plaza, matriculación de alumnos, gestión académica, trámites administrativos, gestión de becas y actividades extraescolares.

En los centros escolares suele existir un fichero, en soporte papel, que está compuesto por los expedientes académicos de cada uno de los alumnos. El *"expediente académico"* es una carpeta personal de cada alumno en el que los centros escolares almacenan toda la información documental relativa al alumno que, en algunos casos, también puede contener certificados médicos, informes psicopedagógicos o aquellos que elabora el tutor correspondiente a cada curso académico que contiene innumerables datos especialmente protegidos por lo que sus seguridad debe ser máxima.

También suele ser común a todos la existencia de un fichero que custodia el departamento de orientación del centro escolar o el Equipo Psicopedagógico de la Consejería de Educación, y que contiene todas las pruebas de evaluación psicopedagógica, entrevistas e informes que realiza el orientador al alumno que lo requiere, en especial, información relativa a alumnos con necesidades educativas especiales.

Se recomienda, en aquellos sistemas de información que traten Datos de Carácter personal en que se utilicen conexiones a Internet, se extremen las medidas de seguridad, para evitar ataques a los sistemas y minimizar la posibilidad de que se produzcan fugas de información.

Se han de tener activados los "firewall" y adoptar toda medida adicional de protección que se considere conveniente ya que una fuga de información podría ser catastrófico, primero a los afectados y segundo al Centro Escolar y la Administración.

Como ya hemos comentado, la tipología de datos que se tratan en los centros escolares y, por extensión, en las Consejerías de Educación, tanto en el sistema de información automatizado como en los ficheros manuales, contiene datos especialmente protegidos, por lo que el nivel de seguridad a aplicar al "Fichero de Alumnos" debe ser ALTO siempre.

Es de vital importancia tener en cuenta estas medidas y aplicarlas para evitar problemas de consecuencias.
Debemos incidir en la necesidad de calificar correctamente los ficheros en función de la naturaleza de los datos tratados, de modo que sean considerados de nivel básico, aquellos que contengan datos de carácter personal, y de nivel alto, los que, además, contengan datos especialmente protegidos.

### 5.9.1 Documento de seguridad

En el artículo 88 sobre El documento de seguridad del Real Decreto 1720/2007 se indica que 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 todo el personal con acceso a los sistemas de información de datos personales.
Este 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 en este caso medidas de seguridad de tipo alto.*
*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.*

De todos estos aspectos hablaremos a continuación dando algunas recomendaciones de actuación y observaciones recogidas en mi práctica profesional como docente.

Al tratarse con datos personales estamos en la obligación de redactar un documento de seguridad al igual que los equipo de orientación de la Consejería Educación de Castilla y León.

Se están tratando con datos especialmente protegidos por lo que es más que obligatoria la redacción del mismo.

Es importante además detallar como se realiza el acceso, que medios, que ficheros quién tiene acceso a los mismos, que tipo de datos se tratan, que medidas de seguridad se toman en función de los datos que tratan. Hacer hincapié en las personas que acceden a los datos de la necesidad de cumplir con las obligaciones de seguridad impuestas por la normativa, máxime cuando se trabaja con datos de todo tipo, incluso especialmente protegidos y de menores de edad.

### 5.9.2 Funciones y obligaciones del personal

Como podemos observar en el plan sectorial redactado por la Agencia Española de Protección de Datos ninguna Consejería de Educación, ha elaborado y distribuido a los centros escolares al igual que en la de Castilla y León.

Tampoco se hace firmar ningún documento a los trabajadores en el que se les imponga el deber de secreto ni sus funciones o formas de actuar con los datos que manejan de carácter

personal por lo que el tratamiento de datos es algo que se hace con la responsabilidad que cada uno tiene a la hora de actuar.

Sería completamente necesario un documento en el que se encuentren definidas las funciones y obligaciones de cada una de las personas que tienen acceso a los datos de carácter personal y a los sistemas de información utilizados para gestionar los datos personales de los alumnos, en los términos establecidos por el Reglamento de Medidas de Seguridad debido a que se pone muy en entredicho el cumplimiento adecuado de la LOPD.

Como la Consejería de Educación no ha distribuido el citado documento ni han adoptado ninguna medida para que el personal conozca las normas de seguridad, el personal de los centros escolares desconoce las normas de seguridad que afectan al desarrollo de sus funciones, así como las graves consecuencias en que pudieran incurrir en caso de incumplimiento.

En la mayoría de los centros escolares, sus representantes, ante la falta de información, apelan a la ética profesional de todos los profesores en el desempeño de sus funciones. Los orientadores también apelan a su ética profesional y a la confidencialidad de la información que tratan.

### 5.9.3 Gestión de incidencias

Como se indica en el artículo 90. Registro de incidencias del Real Decreto 1720/2007 de desarrollo de la LOPD 15/1999 deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal 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 en la resolución del problema.

Los centros escolares al no disponer de documento de seguridad están deficitarios en este aspecto que por lo general solventa la Consejería de Educación a través de su sistema de incidencias informáticas, ya que, en todas las Comunidades Autónomas, el mantenimiento y

la actualización de las aplicaciones informáticas se realiza por parte de personal de la misma, a través de un departamento de atención o gestión de incidencias. Este servicio, sin embargo, no incluyen un procedimiento de gestión y notificación de incidencias en los términos establecidos en el Reglamento de Medidas de Seguridad y, por tanto, los centros escolares tampoco disponen de un registro de incidencias por lo que están incumpliendo la LOPD.

Resulta preciso que tanto los centros escolares como las Consejerías de Educación cuenten con un registro de incidencias, en el que quede constancia el procedimiento de notificación y gestión en el que se haga constar el tipo, el momento de su producción, la persona que realiza la notificación, a quién se le notifica y los efectos que se hubieran producido derivados de la misma.
Los centros escolares están tratando datos especialmente protegidos que exigen medidas de seguridad de tipo alto por lo que es demasiado necesario tener este registro de incidencias, no sólo de tipo informático.

### 5.9.4 Control de accesos

En este apartado, se incluye lo dispuesto por la normativa de protección de datos, en lo referente a la identificación y autenticación, así como todo lo relativo al acceso a los datos personales y al acceso físico a los mismos.

En este aspecto los centros escolares se encuentran muy deficitarios ya que generalmente este registro nunca se produce, los centros no cuentan con procedimientos escritos de asignación, distribución y almacenamiento de las claves de identificación y autenticación para acceder a los sistemas de información que tratan los datos personales de los alumnos, así como tampoco existe una relación de los usuarios que tienen acceso autorizado a dichos sistemas. Es por ello necesario realizar este control de accesos para evitar posibles problemas con los datos.

Por ello es necesario elaborar una relación actualizada de usuarios que tienen acceso a la aplicación utilizada para gestionar los datos personales de los alumnos de manera correcta y

con un control adecuado de a que accede cada uno y a que puede acceder cada uno en función de su puesto de trabajo.

Generalmente los centros escolares disponen de un código de usuario y contraseña para acceder al sistema de información que gestiona los datos personales de sus alumnos que les facilita la Junta de Castilla y León a través de la Consejería de Educación al igual que se produce en el proceso de admisión de nuevos alumnos y de matriculación de éstos.

.

Por otra parte, los centros escolares como desconocen las medidas de seguridad que deben de aplicar no hacen el cambio de contraseñas al que están obligados de manera periódica, incumpliendo con las medidas de seguridad exigidas y facilitando que los datos de los afectados puedan llegar a ser vistos por personas que no deban verlos.

También debe evitarse en la medida de lo posible poner al alcance de todos las contraseñas de acceso al sistema de datos personales evitando así problemas e incidencias de consecuencias imprevisibles.

También debemos velar por que cada usuario de un ordenador del colegio tenga su propia sesión y no pueda acceder a los datos del resto, evitando el intrusismo a información por ejemplo de informes de equipos psicopedagógicos que contienen datos especialmente protegidos.

Es también importante actualizar los datos de las personas que acceden a datos año tras año para incluir a los nuevos y por otra parte eliminar a los que ya no realizan servicios dentro del mismo. También se debería limitar los recursos a los que puede acceder cada usuario dando un acceso a datos en función del puesto que ostente.

Normalmente, en todos los centros escolares únicamente aquellos usuarios autorizados acceden a los datos personales de los alumnos aunque en la realidad son todos o casi todos los que acceden a los datos personales.

Tampoco se encuentra legislado el registro de accesos en los términos recogidos en el

Reglamento de Medidas de Seguridad ni existen procedimientos para dar de baja usuarios que no prestan su servicio en los centros escolares ni tampoco para conceder, alterar o anular accesos a los sistemas de información.

En algunos centros escolares los profesores tienen acceso, únicamente, al sistema de información y a los expedientes académicos de los alumnos a los cuales imparten enseñanza y, en algunos casos, el acceso al expediente académico únicamente está permitido exclusivamente al tutor, no a los profesores. En otros casos, el acceso al expediente académico está permitido a los profesores, a la dirección y al personal administrativo del centro escolar. Por ello es importante homogeneizar el sistema y dejar claro, delimitar que puede hacer cada miembro.

También debería hacer un seguimiento más exhaustivo de la custodia de los datos personales de los alumnos que suelen estar generalmente en la secretaría del centro escolar, sin cerrar bajo llave, lo que permite acceder a los mismos de manera sencilla tanto por docentes y personal del centro como por el resto de personas que no pertenezcan al colectivo de trabajadores.

Como podemos ver en la sección 3ª de medidas de seguridad de nivel alto en el artículo 111 sobre almacenamiento de la información del Real Decreto 1720/2007 los armarios, archivadores u otros elementos en los que se almacenen 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. Este es e caso de los ya hablados expedientes académicos. Además, dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

**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. SECCIÓN 3. ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO ***Artículo 111***. Almacenamiento de la información.
1. 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. 2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad**.**

Por lo general, todos los profesores tienen posibilidad de acceso a los expedientes de alumnos del centro incluso de los que no tutoriza o da clase ya que habitualmente se encuentran todos los expedientes juntos, por lo que si tienes acceso a un expediente, tienes automáticamente acceso al resto de expedientes.

El acceso a los locales donde se encuentran ubicados los sistemas de información con datos de carácter personal debe estar reservado a las personas autorizadas. Así el acceso al archivo de expedientes únicamente debiera estar permitido a aquellas personas que disponen de la llave del archivo, el acceso a las salas donde se ubican los servidores deben estar cerrados con llave, así como los despachos utilizados por el departamento de orientación y tutores que generalmente es normal que se encuentren abiertos. Este aspecto debe ser tenido en cuenta y ser meticulosos por parte de la dirección del centro y los trabajadores para que no se produzcan problemas de pérdida de datos ni sustracción de documentación debido a los problemas que podría ocasionar.

Finalmente añadir que en la mayoría de los centros escolares se dispone de accesos a Internet, desde los ordenadores utilizados para gestionar los datos personales de los alumnos e incluso desde los ordenadores utilizados por los orientadores y como ya hemos indicado anteriormente debería haber sistemas de seguridad como firewall para evitar que se produzcan accesos no autorizados desde el exterior a datos de carácter personal de todo tipo.

Según se dispone en el artículo 24.4 (1) del Reglamento de Medidas de Seguridad se ha de mantener un registro de accesos al sistema, conservándose los mismos al menos dos años, comprobar que las contraseñas se cambian periódicamente y que se siguen normas para hacerlas seguras y por último se recomienda utilizar protectores de pantalla para evitar el acceso al ordenador por parte de terceros no autorizados.

**Real Decreto de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal 994/1999 de 11 de junio** ***Artículo 24***. Registro de accesos.

4. El período mínimo de conservación de los datos registrados será de dos años.

### 5.9.5 **Gestión de soportes**

Los centros escolares disponen de soportes informáticos que contienen datos de carácter personal de los alumnos, aunque, no se disponen de procedimientos que permitan su gestión, ni suelen estar inventariados desde el punto de vista de la normativa de protección de datos.

De forma general, tampoco se dispone de procedimientos de distribución y reutilización de soportes, ni tienen normas al respecto para la reutilización de los soportes, aspecto que debe cambiarse e implantarse en el centro para mejorar y aprovechar los recursos lo mejor posible.
Los centros escolares suelen remitir, en la mayoría de las ocasiones, información a los padres vía correo ordinario, incluso entre centros escolares suele ser ésta la vía de intercambio de información.

Es importante reseñar que, en algunas ocasiones, se trata de informes o listados elaborados por los departamentos de orientación y contienen datos especialmente protegidos, sobre todo cuando hacen referencia a tratamientos y evaluaciones psicopedagógicas de alumnos con necesidades educativas especiales, aspecto a cuidar ya que debemos aplicar medidas de seguridad alta.

También se da el caso de entregas de documentación en mano a la Consejería de Educación, o la utilización de correo certificado, como es el caso de remisión del libro de escolaridad o el expediente académico al centro donde se traslada un alumno.

Respecto a la destrucción de documentos, los centros escolares utilizan distintas vías o procedimientos para ello. Los más habituales son los siguientes:

- Contenedores de papel reciclado de cartón cuya tapa es igualmente de cartón con una ranura, sin ningún tipo de cerramiento, que semanalmente son recogidos por una empresa externa, no realizándose certificados de destrucción de los mismos.
- Máquina destructora de papel instalada en el centro escolar pero cuya existencia no es conocida por todo el personal, lo que no permite garantizar que toda la destrucción de documentación se curse por esta vía.

- Trocear los documentos y depositarlos en la papelera, bien por no disponer el centro escolar de destructora de papel o por desconocimiento de su existencia. En este caso, las papeleras suelen vaciarlas los empleados de la limpieza y, por tanto, lo más probable es que los documentos terminen depositados en un contenedor en la vía pública.
- Finalmente, en algunos centros escolares, los documentos se queman.

Se ha detectado que los profesores de algunos centros escolares se suelen llevar a su domicilio particular los exámenes que realizan sus alumnos para corregirlos. En otras ocasiones, se llevan disquetes con los listados de sus alumnos para incorporar la nota correspondiente a los exámenes de evaluación. En ningún caso, han recibido instrucciones por parte del centro escolar o de la Consejería de Educación sobre cómo proceder en estos casos ya que pueden producirse pérdidas de la información fuera del centro de trabajo.

Especial atención merece el caso de algún orientador del equipo multidisciplinar de la Consejería de Educación, que lleva un disquete consigo en el que se incluye toda la información psicológica de los alumnos que trata sin cifrar, y de un jefe de estudios que se lleva a su domicilio, en disquete o en papel, los listados de todos los alumnos de un ciclo de enseñanza para distribuir los grupos.

Es necesario que todos los soportes informáticos estén inventariados, de manera que sea posible identificar los datos contenidos en ellos. Además se ha de disponer de procedimientos de distribución y reutilización de soportes.
Por lo que se refiere al registro de entrada/salida de soportes, se ha de disponer del mismo en los términos previstos en el Reglamento de Medidas de Seguridad.
Se recomienda que las comunicaciones por correo postal se realicen mediante correo certificado o bien mediante entrega en mano.

Respecto a la destrucción de los documentos, se ha de verificar que la misma se produce de modo que se impida el acceso a los mismos por parte de terceros, y, en el caso de usar empresas externas para realizarlo, se ha de haber suscrito un contrato, que recoja los extremos previstos en el artículo 12 de la LOPD (1), y obtener un certificado de destrucción a tenor de lo pactado.

**(1) Ley orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal**. ***Artículo 12***. Acceso a los datos por cuenta de terceros. 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.

Cuando se vayan a sacar datos de los alumnos fuera del centro escolar, es preciso que quede constancia de ello en el registro de gestión de soportes y que sea autorizada la salida por el responsable del fichero, que fijará además el modo de hacerlo.

### 5.9.6 Copias de respaldo y recuperación

Se debiera de realizar copia de seguridad al menos una vez a la semana a no ser que en ese periodo se hubiera realizado alguna modificación de los mismos, y así para cumplir con el Reglamento de Seguridad; además debiera de haber unas normas o instrucciones para la realización de las mismas que la Administración debiera de facilitar y así homogeneizar el proceso en todos los Centros Públicos de la Comunidad y asegurar que se llevan a cabo de manera correcta las instrucciones del Reglamento de Seguridad.

Por otra parte, estas copias de respaldo deben siempre realizarse en dispositivos externos al ordenador del que proceden y asegurarse de que es legible la información que dentro existe, que el formato en que están guardados los datos es universal y fuera e que fuera el lugar donde accedamos a esos datos con la copia de respaldo podamos acceder sin ningún tipo de problema.

Otro aspecto a cuidar es el lugar de ubicación de las copias de seguridad, evitando lugares que estén al alcance de cualquier persona, estas copias deben estar siempre custodiadas bajo llave y con acceso a la misma solo por el responsable del tratamiento o por la persona o personas autorizadas por éste. Y es que estamos tratando datos de carácter personal de doble vertiente, por una parte datos de alumnos menores de 14 años y por otra parte datos especialmente reservados por lo que las medidas que debemos utilizar deben ser la de tipo alto para todos los soportes como para las copias y todo el material que contengan estos datos personales.

Estas mismas premisas deben ser llevadas a cabo por todas las personas o equipos que dispongan datos de carácter personal sean o no especialmente protegidos. Este es el caso de los departamentos de orientación, que deben realizar copias de respaldo con la misma periocidad, es decir, una vez semanal a no ser que en ese periodo se hubiera realizado alguna

modificación, o en su caso dar esta labor al departamento correspondiente como puede ser el departamento de informática del centro.
Dichas copias se han de custodiar en un lugar diferente a aquel en que se encuentran los equipos informáticos, y se realizarán al menos una vez a la semana, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
Las copias se han de verificar para comprobar que los datos allí almacenados son legibles.

### 5.9.7 Responsable de seguridad

Como se establece en el artículo 95 del Real Decreto 1720/2007 (1) en el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo.
Además, esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, en nuestro caso podemos diferenciar datos con medidas de seguridad alto y datos con medidas de seguridad alto ya que hay datos especialmente protegidos
.
Aún habiendo un responsable de seguridad, el responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento no podrá desligarse de las obligaciones que le corresponden y siempre asumirá las consecuencias de los problemas suscitados en el tratamiento de datos personales.

### 5.9.8 Auditoría

Como se establece en el artículo 110 los ficheros se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.
El Reglamento de Medidas de Seguridad, en el artículo 17 recoge todos los aspectos relativos a la Auditoría en el apartado 1 se especifica que *"los sistemas de información e instalaciones*

**(1)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.* SECCIÓN 2. ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO ***Artículo 95***. Responsable de seguridad.
En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. 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.
En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

*de tratamiento de datos se someterán a una auditoria externa interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años*".

Por ello, deberemos hacer cumplir la auditoría y preparar al centro para evitar sorpresas cuando se realiza la visita por parte de una auditoría.

### 5.9.9 Telecomunicaciones

En el momento en que se realicen envío o traslados de datos personales en el Artículo 104 referido Telecomunicaciones del Real Decreto 1720/2007 cuando, conforme al artículo 81.3 (1) deban implantarse las medidas de seguridad de nivel alto como es nuestro caso al tratar datos especialmente protegidos, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

### 5.9.10 Deber de secreto

En la LOPD en el artículo 10 se indica 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.

Los centros escolares, para el desarrollo de su actividad, necesitan, además de profesores, la colaboración de distintos tipos de profesionales como puede ser psicólogos, pedagogos, logopedas, orientadores escolares o educadores sociales. Asimismo, necesitan de personal administrativo, de limpieza y conserjes. Todos ellos, en algún momento, acceden o pueden tener acceso a los sistemas de información o documentación que contienen datos personales de los alumnos.

**(1)Real Decreto 1720/2007** ***de 21 de diciembre,*** Artículo 81. *Aplicación de los niveles de seguridad.* 3. 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.

El artículo 18 del Real Decreto 732/1995 (1) de 5 de mayo, "Derechos y deberes de los alumnos y normas de convivencia en centros docentes no universitarios", establece que todos los centros docentes estarán obligados a guardar reserva sobre toda aquella información de que dispongan acerca de las circunstancias personales y familiares del alumno. No obstante, los centros comunicarán a la autoridad competente las circunstancias que puedan implicar malos tratos para el alumno o cualquier otro incumplimiento de los deberes establecidos por las leyes de protección de los menores.

Respecto de los profesionales que atienden a los alumnos con necesidades educativas especiales, la Orden de 14 de febrero de 1996 recoge lo siguiente:

"*Los profesionales que, en razón de su cargo, deban conocer el contenido tanto del informe de evaluación psicopedagógica, como del dictamen de escolarización, garantizarán su confidencialidad. Serán responsables de su guardia y custodia las unidades administrativas en las que se deposite el expediente*".

Además en la Ley Orgánica Educativa 2/2006 en su disposición adicional vigésimo tercera, en su apartado 3, se establece que "*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*."

En relación al personal que trabaja en los departamentos de orientación, psicólogos, pedagogos, logopedas, orientadores escolares o educadores sociales, todos ellos deben ser conscientes de que la información de carácter personal que manejan es especialmente sensible ya que incluye diagnósticos, valoraciones y dictámenes profesionales sobre el estado de salud física o psíquica de los alumnos o incluso valoraciones sobre su vida personal y familiar razón por la cual su deber de sigilo debe ser extrema ya por las razones ya mencionadas .

**(1)Real Decreto 732/1995 de 5 de mayo, "Derechos y deberes de los alumnos y normas de convivencia en centros docentes no universitarios**" ***Artículo 18***. Los centros docentes estarán obligados a guardar reserva sobre toda aquella información de que dispongan acerca de las circunstancias personales y familiares del alumno. No obstante, los centros comunicarán a la autoridad competente las circunstancias que puedan implicar malos tratos para el alumno o cualquier otro incumplimiento de los deberes establecidos por las leyes de protección de los menores.

Sería adecuado que la Administración obligara a todo el personal a firmar un documento en el que se comprometan al sigilo o secreto profesional y que además en los soportes en los que haya información de datos personales exista alguna leyenda en la que se indicara la garantía de confidencialidad por parte de los profesionales que necesitan acceder al contenido de los mismos o se incluya únicamente una marca con la palabra "CONFIDENCIAL".

Por otra parte está el personal administrativo, el que realiza las labores de limpieza, los conserjes o monitores que imparten actividades extraescolares, no siempre forman parte de la plantilla de la Consejería de Educación de la Comunidad Autónoma sería conveniente que se remitiera a todo el personal funcionario o laboral que presta servicios en los centros escolares una instrucción en la que se recuerde el deber de sigilo que impone el artículo 10 de la LOPD y la disposición adicional vigésimo tercera de la LOE e incluir en sus contratos de trabajo una cláusula de confidencialidad que recogiera el contenido del citado artículo 10 y así nadie olvidara sus obligaciones.

### 5.9.11 Cesiones de datos

El artículo 11 de la LOPD, en su apartado 1, recoge lo siguiente:
*"1. 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".*

*En el artículo 10 de Real Decreto 1720/2007 se establece que l*os datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello aunque será posible el tratamiento o 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.

Los centros escolares están obligados a ceder datos personales de los alumnos a la Administración, para la realización de determinados trámites impuestos por la legislación educativa por lo legalmente están habilitados para tal cesión. Generalmente, se entregan,

siempre que los solicita la Administración sin conocer el centro educativo que dicha cesión cuente con justificación legal.
No estarán habilitados para tal cesión cuando dan los datos personales a empresas privadas sin el consentimiento expreso del interesado o este caso de los tutores o padres.

Por otra parte podemos hacer alusión a las posibles cesiones de datos que se producen en la práctica diaria de los centros escolares como son:

**Consejería de Educación:**

Los centros escolares entregan a la Consejería de Educación de la Comunidad Autónoma los formularios de solicitud de plaza y la documentación que los acompaña para que las bareme.
Los centros escolares, habitualmente, entregan un ejemplar del formulario de solicitud de plaza y un listado de alumnos no admitidos.

En el proceso de solicitud de becas, los centros escolares hacen de intermediarios entre las familias y el Ministerio de Educación o la Consejería de Educación que las convoca.
Remiten los dictámenes de escolarización, que elabora el departamento de orientación, de alumnos susceptibles de participar en Programas de Garantía Social o de
Diversificación Curricular.

**Consejería de Sanidad:**

Los centros escolares suelen entregar a la Consejería de Sanidad de la Comunidad Autónoma, un listado de alumnos por clase susceptibles, por su edad, de ser vacunados o de programas de reconocimiento médico o revisiones bucodentales por parte de la Consejería de Sanidad en la que se hace control de los alumnos a los que se ha aplicado un tratamiento determinado. También suele haber control con listado de los alumnos a los que semanalmente se les aplica flúor.

Como ya hemos indicado debemos siempre comprobar de manera fehaciente que la cesión es legal y cumple con la normativa al respecto.

**Comisión de Escolarización:**

Algunos centros escolares entregan a la Comisión de Escolarización los formularios de solicitud de plaza escolar debidamente cumplimentados, junto a la documentación anexa como informes psicopedagógicos.
También remiten a la Comisión de Escolarización un listado que contiene los datos personales de los alumnos que se incorporan por primera vez al centro escolar, para que elabore el libro de escolaridad donde se irán anotando las calificaciones de los distintos cursos académicos.

Además se remiten los acuerdos de apertura y la resolución de expedientes disciplinarios tramitados por el centro escolar y listados de aquellos alumnos que, al haber finalizado sus estudios satisfactoriamente.

El departamento de orientación de algún instituto remite a la Consejería de Educación listados con datos personales relativos a minorías étnicas o socioculturales, así como datos de alumnos con necesidades educativas especiales, listados, que además de datos identificativos, incluyen otro tipo de información, como, por ejemplo, la relativa a deficientes psíquicos, trastornos graves de personalidad o hiperactividad (es decir, datos especialmente protegidos).
En estos casos hay que prestar atención a la hora de enviar esta información ya que contiene datos especialmente protegidos y deben estar protegidos por medidas de seguridad alto.

**Otras cesiones:**

En el momento que un alumno se traslada de centro escolar, el de origen suele remitir al centro escolar que escolariza al alumno, el libro de escolaridad y el expediente académico completo, incluyendo los informes psicopedagógicos archivados en el departamento de orientación, sobre todo si se trata de un alumno con necesidades educativas especiales por lo que se debe prestar atención a la hora de hacer el envío de información y asegurarse de que se está haciendo una cesión de manera regular.

.

También existe cesión de datos cuando el colegio envía o cede la información de los alumnos que se matriculan en el instituto y abandonan el centro escolar. Esta información enviada contiene información de todo tipo por lo que como a hemos comentado prestar atención a como se envía y que habilitación legal tenemos para ese envío.

Además, la Consejería de Educación permite a los centros escolares acceder a la información extraída de la Agencia Tributaria de aquellas familias que lo autorizan a efectos de baremación de la solicitud de admisión.

También suelen entregar listados con datos personales, de alumnos o de sus padres o tutores, a la AMPA del centro escolar.

Cuando un centro escolar participa en intercambios internacionales de alumnos, suele remitir, a la entidad organizadora del intercambio, información sobre el perfil familiar y datos personales del alumno. En algunos casos, es el profesor el que incluye dichos datos en la página "web" de la entidad organizadora. En este tipo de cesiones también se está realizando una transferencia internacional de datos que después comentaremos.

Ante visitas a realizar por los alumnos a determinados museos, el centro escolar remite al mismo un listado de los alumnos que van a asistir.
Finalmente, los centros escolares remiten información de alumnos a instancia de los correspondientes Juzgados de Menores.
Las cesiones de datos personales de los alumnos en el proceso de admisión a la
Comisión de Escolarización, están amparadas por la legislación vigente en materia de educación.

Para poder resolver la duda de la habilitación por parte de los centros escolares a realizar cesiones de datos, debemos referirnos a la aplicación de la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006, de 3 de mayo de educación, haciéndose referencia a su apartado 2 ya que la legislación autonómica en la ORDEN EDU/1951/2007, de 29 de noviembre en la disposición adicional primera establece que el tratamiento de los datos personales del alumnado se ajustará a lo dispuesto en la disposición adicional vigésima

tercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos y en sus normas de desarrollo.

En esta disposición adicional se establece, con carácter general, en su apartado 1 que "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".

En el apartado 2 se concreta que "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".
De lo previsto en ambos apartados se desprende la existencia de una habilitación legal para el tratamiento por los centros educativos de los datos de los alumnos y de los relacionados con su entorno familiar y social que sean necesarios para el adecuado cumplimiento de la función educativa, descrita por el apartado 2 en sus vertientes docente y orientadora.

Las comunicaciones que realizan los centros escolares a las Consejerías de Educación de la Comunidad Autónoma, en principio, no pueden ser consideradas como cesiones de datos ya que el responsable de los ficheros y tratamientos es la propia Consejería. Además, los tratamientos que realizan los centros se encuentran amparados por la distinta normativa que regula los procedimientos de admisión de alumnos, la emisión de libros de escolaridad, la gestión de becas, de títulos, o de la prueba de acceso a la universidad.

No obstante, las Consejerías de Educación son organismos en los que el responsable de los ficheros puede ser una unidad concreta de entre todas las que componen la Consejería. En virtud de lo anterior, es importante destacar que no todas las cesiones que se realizan a las

Consejerías de Educación puedan resultar amparadas por la legislación vigente ya que el receptor de los datos personales, puede ser diferente al responsable del fichero.

Algunas de las cesiones citadas podrían estar amparadas por otro tipo de legislación, como es el caso de las comunicaciones realizadas a los Juzgados de Menores, en virtud de la Ley Orgánica 5/2000, reguladora de la responsabilidad penal de los menores, y en la que se recoge, incluso, la información que deben contener los informes remitidos.
En el resto de las cesiones mencionadas, es preciso analizar si hay habilitación legal para ello ya que, en caso contrario, no se pueden realizar si no se dispone del consentimiento exigido por la normativa de protección de datos, salvo que la comunicación se realice a un encargado del tratamiento.

Finalmente, añadir que los centros escolares, habitualmente y apoyándose en el principio de colaboración entre administraciones, suelen remitir cualquier tipo de información que se les solicitan. Entre la información que facilitan se incluyen datos especialmente protegidos cuando, en este caso, sería necesario contar, si no existe habilitación legal, con el consentimiento expreso de los afectados.
Por tanto, en este apartado, la recomendación debe ser que cada centro escolar revise las cesiones que realiza para analizar, en cada caso, si la misma dispone de habilitación suficiente desde el punto de vista de la normativa de protección de datos de carácter personal.

### 5.9.12 Prestación de servicios

Los centros escolares, en algunas ocasiones, necesitan acudir a terceras empresas o profesionales para que les presten determinados servicios.

Como se indica en el artículo 12 de la LOPD *"Acceso a los datos por cuenta de terceros"*, recoge lo siguiente:

> *"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."*

Con carácter general, los centros escolares acuden a terceras empresas para que les presten los servicios que se exponen a continuación, teniendo en cuenta que los mismos son contratados directamente por los centros escolares, la AMPA o la Consejería de Educación. Algunas de estas terceras empresas con las que se realizan cesiones de datos son por ejemplo:

- Los gabinetes fotográficos, que elaboran la orla, bien por encargo de los centros escolares o de la AMPA, tienen conocimiento del nombre y apellido de cada uno de los alumnos que son fotografiados.
- El servicio de transporte escolar entre el domicilio y el centro que prestan empresas externas suele ser contratado directamente por la Consejería de Educación, a la cual el centro escolar debe remitirle el listado de alumnos que han solicitado este servicio para que ésta se lo entregue a la empresa.
- El servicio de reparación y mantenimiento de la red informática suele prestarlo directamente la Consejería, aunque, en algunos casos, acude a los servicios técnicos

de terceras empresas al igual que ocurre con el mantenimiento del "software", que utilizan los centros escolares para el tratamiento de los datos personales de los alumnos.

- Los centros escolares contratan los servicios de empresas externas para que impartan actividades extraescolares. En algunas ocasiones, la encargada de proponer y contratar dichos servicios es la AMPA del centro.
- El servicio de guardería o "madrugadores", que es la atención a aquellos alumnos que acuden al centro antes de comenzar la jornada escolar, y el servicio de comedor, es contratado a una empresa externa bien por el centro escolar bien por la AMPA.
- Una empresa externa es la encargada de recoger el papel inservible en aquellos centros escolares que han instalado contenedores en sus dependencias. Lo mismo ocurre cuando se trata de ordenadores o material informático no reutilizable.
- Imprentas y servicios de encuadernación cuando se realizan revistas escolares del centro escolar con nombres y apellidos de los alumnos y profesores del centro e imágenes de los mismos.
- Finalmente, en algunos casos, los centros escolares son los encargados de realizar las labores administrativas a la AMPA, tales como la emisión de recibos o la elaboración de etiquetas con los datos personales de los padres o tutores de los alumnos.

Los centros escolares deben revisar si se hace mención al artículo 12 de la LOPD y que se firma un contrato de servicios en el que a empresa tercera se comprometa a cumplir con los preceptos de la normativa de la LOPD.

Se debe establecer un contrato en el que se recojan los servicios que se van a realizar y las obligaciones que se suscriben cumpliendo en especial con el apartado 2 y 3 del artículo 12 de la LOPD (1).

**(1) LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal**. ***Artículo 12*** 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.

## 6. IMPLANTACIÓN DE LA PROTECCIÓN DE LA LEY DE DATOS PERSONALES EN CENTROS ESCOLARES PRIVADOS-CONCERTADOS

Como se indica en el artículo 116 de la Ley Orgánica Educativa 2/2006 de 3 de los centros privados que ofrezcan enseñanzas declaradas gratuitas en esta Ley y satisfagan necesidades de escolarización, en el marco de lo dispuesto en los artículos 108 y 109, podrán acogerse al régimen de conciertos en los términos legalmente establecidos. Los centros que accedan al régimen de concertación educativa deberán formalizar con la Administración educativa que proceda el correspondiente concierto.

### 6.1 Principios de información y consentimiento

El artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD) recoge que *"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".*

Por otra parte, el artículo 5.1, relativo al derecho de información en la recogida de datos, establece que *"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".*

Como se desprende de este artículo debemos incluir en todos los formularios de recogida de datos cláusulas informativas que cumplan con el artículo 5 (1) de la LOPD. Además, debemos recabar el consentimiento para esa recogida de datos que se produce desde el momento en que una familia está interesada en matricular a un hijo/a en un centro escolar privado-concertado.

Respecto del derecho de información, los centros escolares privados concertados de la Comunidad Autónoma de Castilla y León recaban datos personales de los alumnos o de sus familias en las mismas situaciones; cuando se solicita plaza escolar, durante el proceso de matriculación, para realizar gestiones diversas, como puede ser la gestión de la expedición de libros de escolaridad o de los títulos de graduado en ESO o bachillerato, así como para gestionar las pruebas de acceso a la universidad.

Asimismo, también necesitan conocer datos personales para prestar a los alumnos determinados servicios complementarios, tales como el servicio de comedor o las actividades extraescolares al igual que sucede en los centros escolares públicos.

Los formularios recaban datos personales del futuro alumno y de sus familias y son necesarios para que el centro pueda prestar el servicio educativo solicitado. Posteriormente, continúan recabando datos personales por distintos medios, procedentes de los padres, profesores, tutores y orientadores o incluso terceros, de tal forma que se completa el expediente académico.

**(1) Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal *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 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.

Respecto del principio del consentimiento, los centros escolares privados concertados, desde que reciben por primera vez a los padres o tutores solicitando plaza escolar hasta que éste finaliza sus estudios en el centro o abandona el mismo para continuarlos en otro, necesitan realizar distintos tratamientos con los datos personales de las familias y de los alumnos.

Se utilizan distintos soportes o ficheros informáticos, pero también manejan mucha información en soporte papel, tanto de documentación que ha aportado la familia como listados y documentos que se extraen de los sistemas informáticos, con distintas finalidades, o que elaboran los distintos profesionales que prestan sus servicios en el colegio (orientadores, tutores o profesores).

A continuación se exponen algunos procesos de tratamiento de datos personales por parte de los centros privados-concertados:

- Proceso de admisión de alumnos:

Los centros privados concertados utilizan los formularios normalizados por la Consejería de Educación de la Comunidad Autónoma de Castilla y León que como ya hemos apuntado en apartados anteriores cumplen con el artículo 5 y 6 de la LOPD.

- Proceso de matriculación:

Dentro de este proceso se han observado las siguientes situaciones:

- Centros que utilizan el modelo normalizado por la Consejería de Educación, referente al proceso de admisión, que no incluye ninguna cláusula alusiva al artículo 5 de la LOPD y, sin embargo, el formulario de matriculación elaborado por el centro escolar sí incluye información relacionada con el citado artículo, aunque dicha información se considera insuficiente, incompleta y en algunos casos, confusa.

- Centros que utilizan el modelo normalizado por la Consejería de Educación, que incluye alguna cláusula informativa alusiva al artículo 5 de la LOPD, pero que, sin embargo no siempre se puede considerar completa. El formulario de matriculación, elaborado por el centro, no incluye información relacionada con el citado artículo, ni comunica a los padres, por otro medio, este tipo de información, y tampoco se incluye en el resto de los formularios utilizados por el centro escolar.

- Centros que utilizan el modelo normalizado por la Consejería de Educación, que incluye una cláusula informativa incompleta relativa al artículo 5 de la LOPD, que, sin embargo, tampoco es subsanada por la implementada por el propio centro escolar.

Proponemos un modelo con el que hacer cumplir los preceptos de la Ley Orgánica de Protección de Datos cumpliendo con el deber de información, consentimiento, y los derechos que el interesado tiene al ceder datos personales:

**Modelo de matrícula propuesto en cumplimiento de la normativa de deber información y consentimiento y ejercicio de derechos**

**MATRICULA DE ALUMNOS DE NUEVO INGRESO CURSO 2010-2011**

**DATOS DEL ALUMNO**

Primer apellido.....……

Segundo apellido…..…..

Nombre.....DNI*.....……

Nacido en.....

Provincia.....…….

Fecha de Nacimiento..... Nacionalidad.....……

Domicilio.....

Código Postal.....……

Teléfono particular…….

Población.....

Colegio anterior…….....….....……

Dirección……Teléfono ó Fax…….……..…...

Localidad……Provincia….……..……..

***Los alumnos mayores de 14 años deben entregar junto con la matrícula, fotocopia de este documento.**

Elaboración Propia

**DATOS DEL PADRE**

Nombre y apellidos.....……

Lugar y fecha de

nacimiento.....Nacionalidad…….DNI.....

.....……

Profesión.....Lugar de trabajo.....…….

Teléfono móvil….....Teléfono de la oficina.....…….

E-mail:.....

**DATOS DE LA MADRE**

Nombre y apellidos.....……

Lugar y fecha de

nacimiento.....Nacionalidad……DNI....

.....……..

Profesión.....Lugar de trabajo.....……..

Teléfono móvil….....Teléfono de la oficina.....……...

E-mail:.....

**DATOS DE MATRICULA**

Curso en el que ingresa: .....

**Comedor:** SI ❙ NO ❙

(El comedor será optativo a partir de (Curso) de Primaria)

Jornada completa: ❙ Media jornada: ❙ □

Mañanas: ❙ Tardes: ❙

Número de Ruta: ……..……..

Parada:…….…….

**Aula Madrugadores/tarde:** Dirigida a los alumnos de Infantil y Primaria.

Deseamos el servicio del aula madrugadores/tarde: SI ❙ NO ❙

Matinal (de 8.00 a.m. a 8.45 a.m.(Ejemplo)) Vespertino (de 5.00 p.m. a 6.00 p.m.( Ejemplo))

xxxxxxxxxxx, a…..... de…..... de 201….

Firma de los padres*

*Por la firma de este documento certifico que conozco y acepto las normas administrativas del colegio.

"El que suscribe, con la firma del presente documento, declara, y consiente expresa e inequívocamente, que ha sido informado por parte del Colegio xxxxxxxxx, en cumplimiento de la normativa vigente en materia de Protección de Datos de Carácter Personal, de las siguientes circunstancias: a) que la información personal, familiar y económica suministrada a este Colegio para formalizar la matrícula del alumno, se incorpora a un fichero cuyo responsable es xxxxxxxxxxxxxx, y cuya finalidad será exclusivamente gestionar adecuadamente y proporcionarle nuestros servicios educativos en el centro y el envío de noticias, avisos, publicidad y ofertas del Colegio, xxxxxxxxxxxxxxxxxx y de las entidades relacionadas con la misma; b) del carácter facultativo a su respuesta a las preguntas que le ha sido planteadas; c) de la posibilidad de ejercitar, en relación con el fichero de referencia, los derechos de acceso, rectificación, cancelación y oposición, mediante carta dirigida al domicilio del Colegio xxxxxxxxxx sito en xxxxxxxxxx.

☐ Por otra parte, y de acuerdo con la normativa vigente en materia de Protección del Menor, le informamos que, con la X señalada, no autoriza a Colegio xxxxxxxxxx a fin de que, en la página Web, anuario, Newsletter y otras publicaciones del Colegio, pueda aparecer información gráfica y escrita de las actividades de dicho centro educativo que incluyan la imagen de su hijo en fotos de grupos o individual, el nombre, curso, edad u otros datos personales, con el exclusivo fin de gestionar las actividades educativas, las publicaciones propias del centro como pueden ser página Web, anuario, Newsletter o cualquier otro tipo de folleto impreso o digital publicado por el colegio o las entidades relacionadas con el mismo, y la notificación de eventos del Colegio. Podrá Ud. retirar la autorización contenida en el presente párrafo en cualquier momento y con efectos a futuro. La retirada de la autorización no afectará a aquellas informaciones ya divulgadas con anterioridad a dicha retirada."

Elaboración Propia

# CÉDULA SANITARIA ESCOLAR

Nombre/Apellidos del alumno_____

## ANTECEDENTES CLÍNICOS

Enfermedades que ha tenido

_____

_____

¿Ha tenido alguna operación?

_____

¿Tiene alguna enfermedad actualmente de forma crónica o persistente?

_____

_____

¿Tiene alergias o reacciones a medicamentos?

_____

_____

¿Tiene alergias o reacciones a algún alimento*?_____ ¿Cuáles?

_____

_____

*Adjuntar informe del médico o pediatra.

¿Necesita algún régimen?

_____

¿Tiene problemas de vista?

_____

Observaciones_____

_____

Medicamentos que usa habitualmente en caso de:

• Dolor de cabeza _____

• Fiebre_____

• Otros_____

xxxxxxxx, a..... de..... de 201….

Firma de los padres*

"El que suscribe, con la firma del presente documento, declara, y consiente expresa e inequívocamente, que ha sido informado por parte del Colegio xxxxxxxxxx, en cumplimiento de la normativa vigente en materia de Protección de Datos de Carácter Personal, de las siguientes circunstancias: a) que la información personal y familiar suministrada a este Colegio mediante el presente documento, se incorpora a un fichero cuyo responsable es xxxxxxxxxxxxxxxxxx, y cuya finalidad será exclusivamente gestionar adecuadamente y proporcionarle nuestros servicios educativos en el centro y el envío de noticias y avisos por parte del Colegio, y de las entidades relacionadas con la misma; b) del carácter facultativo a su respuesta a las preguntas que le ha sido planteadas; c) de la posibilidad de ejercitar, en relación con el fichero de referencia, los derechos de acceso, rectificación, cancelación y oposición, mediante carta dirigida al domicilio del
Colegio sito en xxxxxxxxxxxxxxxxxxxxxx."

Elaboración Propia

- Proceso de gestión de becas:

Los centros privados concertados hacen de intermediarios entre las familias y el órgano convocante de las mismas. Únicamente cumplimentan la parte académica y entregan la documentación, junto a un listado de solicitantes, a la Consejería de
Educación de la Comunidad Autónoma de Castilla y León. En este aspecto, deberemos cerciorarnos que a la hora de transferir las solicitudes con datos personales de todo tipo sea de manera correcta utilizando las medidas de seguridad necesarias propias de los datos que se están tratando.

- Otros tratamientos de datos:

Se producen tratamientos de datos en relación a actividades extraescolares, a la participación en algún concurso o certamen, a la elaboración de listados por cursos que son remitidos al resto de los padres, o, referentes a alguna actividad relativa a ocio desarrollada por algunos padres del centro. Se debe prestar especial atención debido a que no se suele recoger el consentimiento expreso para la cesión de estos datos, es decir, no se cumple con los artículos 5 y 6 de la LOPD.

Generalmente los Centros escolares Privados-concertados suelen utilizar los formularios oficiales de la Consejería de Educación que como ya hemos explicado cumplen con los artículos 5 y 6 de la LOPD.

Otro problema es el relacionado con los formularios de matrícula debido a que cada centro suele elaborar uno propio adecuando la información solicitada a las necesidades del centro. Es en estos formularios en los que debemos hacer hincapié y hacer cumplir los artículos 5 y 6 de la LOPD y hacer mención de los derechos propios de las personas al ser tratados sus datos personales indicando el lugar y responsable del fichero para posibles ejecuciones de los mismos.

Respecto del resto de los formularios utilizados por los centros privados concertados, como ya hemos repetido en varias ocasiones debe incluirse una referencia completa al principio de información, recogido en el precitado artículo 5.1.

Generalmente, la solicitud de datos personales por parte de los centros privados concertados y la entrega de los mismos por parte de las familias, suele ser una práctica tan habitual y generalizada que ambas partes creen que es un proceso natural que se encuentra amparado por la legislación educativa. Esto, unido al desconocimiento de la normativa de protección de datos, lleva a los centros a solicitar únicamente autorización a los padres para realizar aquellos tratamientos cuya autorización es obligatoria por imperativo legal, cuando precisamente, en tales casos, no es necesario contar con el consentimiento del afectado.

### 6.2 Principio de calidad

El principio de calidad viene regulado en el Título II de la LOPD, artículo 4 y según se recoge en el mismo, *"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"*.

Además, estos datos no podrán utilizarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos, deben ser exactos y cancelados cuando dejen de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Atendiendo a lo anterior, en este apartado se han estudiado los distintos momentos en que los centros escolares privados concertados recaban datos personales, tanto de los alumnos como de sus familias, para analizar su tipología y valorar si pueden ser considerados adecuados, pertinentes y no excesivos en función del tratamiento posterior que va a realizarse con los mismos. También se analizan los datos personales que almacenan, la antigüedad y si disponen de procedimientos de cancelación o bloqueo de los mismos.

A continuación analizaremos los distintos momentos en los que se recogen datos a los interesados como son:

- Solicitud de plaza escolar
- Proceso de matriculación
- Gestión del expediente académico
- Otros formularios de recogida de datos

**Solicitud de plaza escolar**

En la Comunidad Autónoma de Castilla y León, para solicitar plaza en un centro privado concertado, los padres o tutores de los alumnos deben cumplimentar un formulario normalizado por la Consejería de Educación que se publica anualmente. En este curso el formulario de admisión puede ser descargado a través de la Web de la Consejería de Educación de la Comunidad y proceder después a la entrega en un Centro escolar privado-concertado para que como ocurre en un centro público se vayan publicando los listados de alumnos admitidos, no admitidos y excluidos y se proceda después a la matriculación de éstos en el correspondiente Centro Escolar.

Como se indica en el Artículo 84.4 (1) de la Ley Orgánica de Educación de 2/2006 de 3 de mayo de Educación la Administraciones educativas podrán solicitar la colaboración de otras instancias administrativas para garantizar la autenticidad de los datos que los interesados y los centros aporten en el proceso de admisión del alumnado.

Además. Como se refleja en el apartado 8 (2) del artículo 84 de la citada Ley, el procedimiento inicial de admisión se realizará al comienzo de la oferta del curso que sea objeto de concierto y que corresponda a la menor edad. Procedimiento que se realizará de acuerdo con lo establecido para los centros públicos.

La información de carácter tributario que se precisa para la acreditación de las condiciones económicas a las que se refieren el artículo 84.10 (3) de esta Ley, será suministrada

**(1) Ley Orgánica de Educación de 2/2006 de 3 de mayo de Educación *Artículo 4***. Las Administraciones educativas podrán solicitar la colaboración de otras instancias administrativas para garantizar la autenticidad de los datos que los interesados y los centros aporten en el proceso de admisión del alumnado. (2) **Ley Orgánica de Educación de 2/2006 de 3 de mayo de Educación *Artículo 8*** En los centros privados concertados, que impartan varias etapas educativas, el procedimiento inicial de admisión se realizará al comienzo de la oferta del curso que sea objeto de concierto y que corresponda a la menor edad. Este procedimiento se realizará de acuerdo con lo establecido para los centros públicos. (3) **Ley Orgánica de Educación de 2/2006 de 3 de mayo de Educación. Artículo 10** La información de carácter tributario que se precisa para la acreditación de las condiciones económicas a las que se refieren el artículo 84.2 de esta Ley, será suministrada directamente a la Administración educativa por la Agencia Estatal de Administración Tributaria y por los órganos competentes de la Comunidad Autónoma del País Vasco y la Comunidad Foral de Navarra, a través de medios informáticos o telemáticos, en el marco de colaboración que se establezca en los términos y con los requisitos a que se refiere la disposición adicional cuarta de la Ley 40/1998, de 9 de diciembre, del Impuesto sobre la Renta de las Personas Físicas y otras Normas Tributarias, y las disposiciones que las desarrollan.

directamente a la Administración educativa por la Agencia Estatal de Administración Tributaria a través de medios informáticos o telemáticos, en el marco de colaboración que se establezca en los términos y con los requisitos a que se refiere la disposición adicional cuarta de la Ley 40/1998, de 9 de diciembre, del Impuesto sobre la Renta de las Personas Físicas y otras Normas Tributarias, y las disposiciones que las desarrollan.

Los datos que habitualmente se solicitan son los siguientes:

- Datos identificativos básicos del alumno y de los padres o tutores.
- Datos de proximidad domiciliaria familiar o laboral.
- Existencia de hermanos en el centro.
- Título de familia numerosa.
- Importe de la renta anual de la unidad familiar.
- Situaciones de discapacidad física, psíquica o sensorial de alguno de los miembros de la unidad familiar.
- Enfermedad crónica en el alumno.
- Información relativa a necesidades educativas especiales del alumno.

Además, junto a la solicitud de admisión, se debe acompañar diversa documentación:

- Certificado de empadronamiento o certificado laboral de la empresa del padre/madre o tutor.
- Certificado que acredite la renta anual de la unidad familiar, o modelo de autorización para su consulta a la Agencia Estatal de Administración Tributaria.
- Certificado médico, en caso de discapacidad o enfermedad crónica.
- Copia del libro de familia o, en su caso, DNI del alumno.
- Certificado de familia numerosa, en su caso.

Algunos centros tienen concierto para una parte de las enseñanzas que imparten y para otra parte funcionan como un colegio privado, lo que conlleva que, para solicitar plaza en las

enseñanzas no concertadas, los centros recaban datos personales del futuro alumno y su familia a través de formularios elaborados por el propio centro escolar, por lo que se deberá cumplir con los artículos 4, 5 y 6 de la LOPD.

Dentro del tratamiento de datos personales podemos observar que algunos Centros incluyen los datos del formulario de solicitud de plaza de enseñanza privada concertada en un programa, que distribuye la Consejería de Educación a todos sus centros para calcular los puntos obtenidos después de baremar las solicitudes y extraer los listados de admitidos y excluidos.

Como ya hemos indicado, estos programas son accesibles a través de la página "Web" de la Consejería en algunas o a través de un disquete con el programa de gestión facilitado por la Consejería.

En el caso de los datos personales solicitados en formularios de solicitud de plaza para enseñanzas no concertadas se incluyen en los sistemas informáticos propios del centro.

Otros Centros incluyen los datos en un fichero automatizado del propio centro, que les permite gestionar las solicitudes y conservar los datos personales de los alumnos que no obtienen plaza de forma indefinida. Este programa suele ser independiente del que utiliza el colegio para gestionar los datos personales de los alumnos matriculados.

En otros Centros se dispone de un fichero para gestionar todos los datos personales de sus alumnos donde se van añadiendo distintos datos.

En este proceso de admisión los Centros remiten toda la documentación a la Consejería, en la que se bareman las solicitudes de plaza y se elaboran las listas de admitidos y excluidos; después se remiten a los colegios para su publicación en el tablón de anuncios del centro.

Respecto a la cancelación de los datos en los sistemas informáticos:

- Como ocurre en los Centros Públicos, se desconoce si existen procedimientos de cancelación de los datos de los Programas facilitados por la Consejería, no existen órdenes ni legislación al respecto.
- Lo mismo ocurre en los centros, que utilizan programas que facilita la Consejería mediante el envío de un disquete y que lo devuelven con los datos personales de los solicitantes, desconocen cómo procede, en su caso, la Consejería en materia de cancelación de datos.

Cuando se utilizan programas propios por parte de centro para gestionar las solicitudes de plaza la cosa es peor y se suelen mantener indefinidamente los datos, principalmente por el desconocimiento por parte del responsable del tratamiento.

Como podemos observar existe una absoluta carencia de criterio a la hora de considerar un dato personal, recogido durante el proceso de admisión, como no necesario y proceder, en consecuencia, a practicar su cancelación por lo que como ya hemos apuntado convendría que la Comunidad Autónoma dictase unas instrucciones en relación al proceso de archivo y mantenimiento de datos referentes al proceso de admisión de alumnos, ya que los centros escolares desconocen qué funciones deben realizar en relación a este asunto.

**Proceso de matriculación**

Los centros privados concertados suelen utilizar sistemas informáticos para gestionar los datos personales que recogen durante el proceso de matriculación. Además de incorporar los datos personales de sus alumnos en su fichero de gestión, incorporan, además, en el sistema informático de la Consejería de Educación de la Comunidad Autónoma para que la Consejería tenga constancia de los alumnos matriculados en el Centro Escolar.

Al igual que los Colegios público, los Centros privados concertados entregan un formulario de matriculación elaborado por el propio centro que suele recoger información muy similar a la del cuestionario de admisión del alumno al centro que proporcionaba la propia Consejería. Este formulario es el mismo para matricular a todos los alumnos.

En el formulario se solicitan datos básicos del alumno, así como datos de contacto de los padres o tutores, datos de domiciliación bancaria y sobre servicios adicionales, como comedor, pertenencia a la Asociación de Padres y Madres de Alumnos, mutualidad, seguro escolar y servicio de guardería. En algunas ocasiones, se recaban también datos referentes a los estudios de los padres o tutores, profesión, empresa donde trabajan, fecha de nacimiento, y datos personales de los hermanos que no estudian en el mismo centro y que son algunos datos que pudieran ser excesivos e incumplirían el artículo 4 de la LOPD de Calidad de los datos. Es por ello necesario revisar que tipo de información se solicita y si es realmente necesaria para el desarrollo de la función educativa. Por ello, convendría homogeneizar los datos que se solicitan durante el proceso de matriculación de alumnos, con el fin de que no se produjeran dichas situaciones.

Suele ser habitual que los datos personales permanezcan indefinidamente en el fichero de gestión del centro para atender ulteriores peticiones de certificaciones académicas, e incluso la documentación de aquellos alumnos que no han concluido sus estudios en el colegio por trasladarse a otro para continuar los mismos.

Como ya hemos indicado en el apartado anterior, los colegios incluyen los datos personales de los alumnos en ficheros de la Consejería de Educación de su Comunidad Autónoma, desconocen si existen procedimientos de cancelación.

Respecto de la documentación aportada por los padres en los procesos de matriculación, los Centros la conservan durante un año en secretaría y luego la desechan, utilizando una destructora de papel, o simplemente se depositan en una papelera o la en el expediente académico.

Los datos incluidos en los formularios de matriculación se incluyen en los sistemas informáticos, bien del propio centro privado concertado o también en el de la Consejería, pero en ambos casos no existe una política de cancelación de los mismos, por lo que se conservan indefinidamente. En el caso de la documentación anexa, los centros no conocen cómo deben actuar en relación a la misma. Por ello se hace necesario tanto en centros público como privados-concertados que se homogenice el proceso de cancelación de los datos tanto el el periodo de admisión como el en el proceso de matriculación de los alumnos.

**Gestión del expediente académico**

El expediente académico suele ser un fichero, en soporte papel, que se inicia cuando un alumno se matricula en el centro. Consta de una carpeta que identifica a cada alumno y contiene la documentación generada en los procesos de solicitud de plaza, y de matriculación.

Posteriormente, se incorporan todos aquellos informes y documentos que se van generando mientras permanece el alumno en el centro. Entre los documentos incluidos en el expediente académico se encuentran las fotografías del alumno, el libro de escolaridad, las calificaciones obtenidas durante los distintos cursos académicos, los informes de tutoría y, en algunos casos, la ficha de examen de salud y documentos de autorización firmados por los padres o tutores para salidas extraescolares.

Asimismo, también se han observado algunos casos en los que en el expediente académico se incluye documentación antigua relativa a ingresos de la unidad familiar, así como otro tipo de documentación que, relativa al proceso de admisión de alumnos, documentación que en principio ya no es necesaria porque el periodo de admisión ya terminó en el momento en que está matriculado el alumno en el centro escolar.

Debe revisarse que es lo que se incluye y que es lo que no dentro de estos expedientes y destruir la documentación que ya es necesaria porque ya ha cumplido la función para la que fue requerida y que por consiguiente debe ser destruida y no conservada en los expedientes. Éste es el caso de documentación en el proceso de matriculación y da admisión o de resoluciones de expedientes disciplinarios que ya han preescrito y que aun así siguen conservándose.

Cuando un alumno procede de otro centro escolar, toda la documentación que se recibe de aquel también se incorpora al expediente académico.

En los centros privados concertados, los departamentos de orientación custodian un fichero con los expediente elaborados, que contienen las pruebas psicopedagógicas realizadas por los orientadores, así como fichas en las que se recoge información de las entrevistas realizadas con los padres o tutores. Las pruebas realizadas a los alumnos, así como los informes de

resultados, suelen incorporarse a ficheros automatizados ubicados en dichos departamentos no extremando las medidas de seguridad al tratar datos especialmente protegidos.

En otros centros no incluyen los informes psicopedagógicos en el expediente académico, pero sí incluyen algunos informes relativos a las evaluaciones psicológicas y de progresión académica que realiza el departamento de orientación a todos los alumnos del colegio. Debiera dividirse en función del tipo de datos y a las medidas de seguridad necesarias para cumplir con la legislación.

Los centros privados concertados suelen incluir los datos personales, recabados en los documentos que conforman el expediente académico, en el sistema informático del centro por tiempo indefinido no respetando el Reglamento de Seguridad al respecto.
Respecto de la documentación en soporte papel, podemos observar que:

- Centros privados concertados que conservan en el expediente académico toda la documentación, en soporte papel, desde que el alumno ingresa en el colegio. En los colegios en los cuales se incorporan las resoluciones relativas a los expedientes disciplinarios, también se mantienen por tiempo indefinido a pesar de haberse superado los plazos legales establecidos para su prescripción como ya hemos indicado.
- Centros privados concertados que, cuando un alumno cambia de centro escolar, remiten al nuevo el libro de escolaridad y destruyen la documentación del expediente académico, a excepción de las calificaciones que quedan automatizadas en el sistema informático del colegio para poder emitir certificaciones.
- Centros que, cuando el alumno finaliza sus estudios o cambia de centro, remiten el expediente académico y en el sistema informático queda marcado el alumno como "pasivo", no cancelando en ningún momento la información.
- Centros privados concertados que, cuando un alumno finaliza sus estudios o cambia de centro escolar, destruyen del expediente académico en papel toda aquella documentación que no es necesario conservar, custodiando indefinidamente las actas con las notas de las Pruebas de Acceso a la Universidad y el Extracto del Registro Personal del alumno.

Respecto de los expedientes de los departamentos de orientación, éstos suelen utilizar un expediente en soporte papel, que se nutre de aquella documentación que se genera de la relación que mantiene el orientador con los alumnos (pruebas de valoración, resultados, informes emitidos e información recabada de padres o tutores, familia y profesores). También se incluyen informes externos (de servicios médicos, de logopedia, de gabinetes psicológicos, etc...) que aportan los padres o tutores al orientador. Con respecto a estos departamentos, destacamos que los:

- Departamentos de orientación que no utilizan ninguna herramienta electrónica para generar sus informes, conservando toda la documentación en soporte papel (Atención a las medidas de seguridad utilizadas al respecto).
- Orientadores que disponen de un ordenador, compartido con otros profesionales del centro, y que se utiliza para elaborar informes. No suelen cancelar esta información, a pesar de tratarse de un ordenador compartido (Se debe limitar y autenticar los usuarios y limitar los recursos a los que cada uno puede acceder).
- Departamentos que custodian la información durante la permanencia del alumno en el centro y durante los tres o cuatro años siguientes, transcurridos los cuales, se destruye (Atención al Reglamento de Seguridad y los plazos legales de 2 años).
- Departamentos que conservan indefinidamente la información, no habiéndose planteado la eliminación de ningún documento.

Como ya hemos indicado y al igual que los Centros Públicos, los Centros privados concertados no se ha implantado una política de cancelación de los datos tratados en el sistema informático, por lo que suelen disponer de ellos indefinidamente.

Asimismo, tampoco están previstos procedimientos de cancelación en los expedientes académicos y expedientes del departamento de orientación en soporte papel, por lo que, en la mayoría de los casos, se conservan a lo largo de los años.

Como cuestión previa es necesario resaltar que resulta innegable la necesidad de que exista un expediente académico del alumno, en el que se recoja la gestión académica y administrativa de cada uno. Ahora bien, se desconoce cuál ha de ser su contenido exacto, y, por ello, en algunos casos, se incluyen datos especialmente protegidos o datos referentes al

proceso de solicitud de plaza. Por tanto, convendría definir el concepto, naturaleza y contenido del expediente académico, así como los procesos de archivo y, en su caso, eliminación del mismo. Debiera homogeneizarse en toda la Comunidad el contenido del mismo.

**Otros formularios de recogida de datos**

Todos los centros privados concertados, además, de los formulados citados anteriormente, suelen utilizar otros de distinta índole que les permite gestionar los servicios asociados a su labor educativa (servicio de transporte, comedor, guardería, actividades extraescolares o para adherirse a la asociación de padres y madres de alumnos).

Algún centro ha diseñado un formulario, al que se accede a través de su página "Web", para que lo cumplimenten aquellas familias que desean obtener información. Este formulario recaba datos personales relativos a edad, sexo, localidad y provincial, correo electrónico, profesión y estudios.

Estos formularios se suelen elaborar por el propio centro pero, en algunas ocasiones, se trata de formularios propios de la empresa contratada que son entregados a las familias.
Respecto del tratamiento que dan los centros a los datos recogidos en estos formularios, existe una gran variedad de posturas ya que, en su inmensa mayoría, no suelen automatizarse y, si lo hacen, la información suele mantenerse en los ordenadores de forma indefinida. En otros casos, los formularios se entregan a las empresas que gestionan los servicios propuestos, por lo que el centro escolar desconoce qué tratamiento realiza la empresa con los datos recogidos.

Otros colegios, habitualmente, custodian los formularios o documentos durante el curso escolar y luego, o bien los desechan en contenedores, se tiran a la papelera o bien se conservan en el centro escolar mientras el espacio físico lo permita.

Con carácter general, los centros privados concertados elaboran formularios en los que solicitan datos personales que se consideran adecuados, pertinentes y no excesivos en relación con la finalidad para la que son recabados. No cabe concluir lo mismo respecto de

algunos formularios (vía "Web"), utilizados para recabar información del centro, en los que se recogen datos excesivos y no adecuados desde el punto de vista de la normativa de protección de datos (por ejemplo edad, sexo o profesión).

Se ha detectado que los mismos centros escolares que recogen datos que, en principio, se consideran adecuados, pertinentes y no excesivos, no han informado a los afectados del proceso de cancelación de los mismos. Por ello, se hace necesario que subsanen esa carencia, a la mayor brevedad posible, a tenor del principio de información recogido en la normativa de protección de datos de carácter personal.

### 6.3 Derechos en materia de protección de datos

La legislación en materia de protección de datos de carácter personal reconoce a las personas una serie de derechos (acceso, rectificación, cancelación y oposición), recogidos en los artículos 15 y 16 (1) de la LOPD, y los responsables de los centros privados concertados deben estar en disposición de atender, en tiempo y forma, estos derechos.

Al tratarse de datos personales en los que el responsable es el titular del Centro Escolar, deberemos indicar en los formularios de recogida de información a quien deben dirigirse para poder ejercer sus derechos y que derechos se les reconocen a los afectados.

Los centros escolares privados-concertados que siguen el modelo propuesto por la Consejería de Educación cumplen con la normativa ya que como hemos visto en el formulario que proporciona la Consejería, se informa de la finalidad de la recogida de datos y además se indica dónde y ante quién deben reclamar los derechos que les asisten.

**(1) Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter personal** ***Artículo 15.*** Derecho de acceso. 1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes**.** ***Artículo 16.*** Derecho de rectificación y cancelación. 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado**.**

En el caso de estos Centros debemos remarcar que los datos tienen una doble vertiente, la primera, datos de titularidad pública en la que el responsable es la Consejería de Educación y otra vertiente que es los datos pertenecientes a titularidad privada en la que el responsable del fichero es el titular o responsable del tratamiento de los datos personales. En este caso nos debemos dirigir a este responsable y a la dirección física de la que nos deben informar cuando hacen la recogida de datos.
Generalmente los alumnos y padres/madres/tutores de alumnos desconocen los derechos recogidos en los artículos 15 y 16, de tal forma que desconocen la posibilidad de ejercerlos, dónde y a quién pueden dirigirse. Estos centros no suelen disponen de un procedimiento por escrito que les permita atender estos derechos.

Es por ello necesario que se habilite un procedimiento con el que los interesados o representantes de éstos puedan ejercer los derechos que les asisten. Además sería conveniente que fuera un procedimiento homogéneo propuesto por la Administración al tratarse de Centros financiados con fondos Públicos.

Ante tal desconocimiento por parte de los afectados, la mayoría de los centros seguramente no suelen recibir solicitudes en los términos recogidos en estos artículos.
Cuando los padres o tutores desean que sus datos personales o los de sus hijos sean modificados por el centro, suelen acudir a la secretaría del mismo y solicitarlo de forma verbal, y, en caso de que la modificación solicitada pueda materializarse, se realiza en el momento, por lo que se puede decir que el ejercicio de los derechos se realiza pero no como indica la legislación en los artículos 15 y 16 de la LOPD.

### 6.4 Inscripción de ficheros

En el artículo 26.1 de la LOPD se recoge que *"toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos"*.

En este epígrafe se trata de hacer cumplir la ley por parte de los responsables de los ficheros, utilizados por los centros privados concertados para gestionar los datos personales de los alumnos notificando los ficheros de datos personales al Registro General de Protección de

Datos y evitando sanciones que en este caso corresponderían al Centro Educativo y no a la Administración como ocurre en los Centros Públicos.

Los ficheros que se inscriban deberán cumplir los preceptos en función del tipo de datos personales que sean, es decir, hacer diferencia entre los ficheros con datos personales con datos especialmente protegidos del resto.

En los ficheros en los que haya datos especialmente protegidos deberemos hacer cumplir medidas de tipo alto y aquellos datos en los que no haya datos especialmente protegidos se deberán aplicar medidas de tipo básico.

Debemos reiterar y concienciar a los centros privados concertados en la obligación de inscribir en el Registro General de Protección los Datos de todos los ficheros con los que gestionan los datos de sus alumnos.

Además, sería correcto insistir en segregar los datos personales especialmente protegidos en ficheros específicos, respecto de los cuales se aplicarán las medidas de seguridad de nivel alto.

### 6.5 Datos especialmente protegidos

En la LOPD se define en el artículo 7 como datos especialmente protegidos los relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual.

En este artículo se recoge en sus apartados 1, 2 y 3 lo siguiente:

> *"1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.*

*2. 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.*
*3. 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".*

Como son muchos los datos especialmente protegidos con los que tratan los Centros Privados-Concertados los iremos explicando detenidamente:

- Respecto al tratamiento de los datos de salud:

Se suelen guardan en los expedientes académicos los certificados médicos de los alumnos algo que debemos cuidar porque no son lo mismo el apellido de una persona que la salud de la misma.

Se debe asegurar, que los informes médicos, psicopedagógicos y los dictámenes de escolarización, que se puedan haber recabado de alumnos con necesidades educativas especiales, se tratan en el sistema de información del centro con el consentimiento expreso de los padres o tutores, o, en su caso, de los afectados.

- Cuando un tutor detecta que un alumno debe ser objeto de atención educativa especial, se pone en contacto con los padres o tutores para informarles verbalmente. Se debe extremar el proceso de tratamiento de estos datos siguiendo la legislación t siempre usando documentos escritos en los que el afectado o interesado firme la autorización expresa para el tratamiento de la información por otras personas.

Para otros procesos médicos como la vacunación o tratamientos médicos como los bucodentales siempre debe recabarse el consentimiento expreso del afectado para poder llevarlos a cabo.

En otras ocasiones se comunica a los padres o tutores la realización de alguna prueba de manera oral o por escrito pero sin incluir una cláusula informativa como se recoge en el artículo 5 de la LOPD, no recabando el consentimiento expreso del interesado.

Otras pruebas realizadas a alumnos a incluir en un programa de diversificación curricular, son diagnosticadas, mediante el empleo de test de inteligencia y habilidades sociales, utilizando un programa informático o similares y no se informa a los padres/tutores de la realización de dichas pruebas, ni se recaba el consentimiento expreso para tal desarrollo de las misma incumpliendo los artículos 5 y 7 de la LOPD.

Por ello se insiste a los Centros privados-concertados en la necesidad de hacer cumplir los artículos 5 y 7 de la LOPD y evitar así posibles molestias y contratiempos al no haber aplicado correctamente la legislación al respecto.

### 6.6 Medidas de seguridad

Con este apartado se analizan las medidas de seguridad aplicadas en los centros escolares Privados- Concertado con los datos de los interesados y como desarrollan el Reglamento de Seguridad indicando y aconsejando como debe realizarse el desarrollo legislativo para cumplir con la legislación al efecto.

Como se indica en el TÍTULO VIII de las medidas de seguridad en el tratamiento de datos de carácter personal en el CAPÍTULO I en sus Disposiciones generales en el artículo 79 (1) los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cuál sea su sistema de tratamiento"

Se describen a continuación y siguiendo las premisas más relevantes desde el punto de vista del Reglamento de Medidas de Seguridad para los centros privados concertados.

**(1) 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**. TÍTULO VIII De las medidas de seguridad en el tratamiento de datos de carácter personal CAPÍTULO I Disposiciones generales

***Artículo 79***. Alcance. Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

### 6.6.1 Sistemas de información

Al igual que en los Centros escolares públicos, los centros privados concertados utilizan programas informáticos para tratar los datos personales de sus alumnos, en unos casos facilitados por la Consejería de Educación para la gestión de la admisión de alumnado como a la hora de matriculación.

La Consejería de Educación además, proporciona programas informáticos, que permiten a los centros baremar las solicitudes de admisión y remitir a la Consejería los datos referentes al citado proceso tanto en los Centros Públicos como Privados.

Así mismo, como ya hemos señalado anteriormente la Consejería de Educación de Castilla y León concede vía Internet un programa informático para gestionar los datos personales de sus alumnos en el proceso de admisión y matriculación en la que cada centro tiene su propia clave de usuario con los datos propios de cada centro.

En la gestión de datos académicos cada centro suele utilizar un Programa elaborado o comprado por ellos mismos.

Como se produce en los Centros Públicos, es común la gestión de un fichero en soporte papel, en el que se incluye los expedientes académicos de cada uno de los alumnos.
Por otra parte, el departamento de orientación suele custodiar en soporte papel las pruebas de evaluación psicopedagógica, entrevistas e informes elaborados por los mismos correspondientes a los alumnos que tratan y que contienen datos especialmente protegidos que no suelen reunir las medidas de tipo alto necesarias para el tipo de datos tratados.

Los sistemas de información que posean los centros privados concertados han de permitir que, en función de la naturaleza de los datos tratados, se respeten las medidas recogidas en el Reglamento de Medidas de Seguridad y que por experiencia propia no reúnen.

Así mismo, en los sistemas de información en que se utilicen conexiones a internet, que se extremen las medidas de seguridad, para evitar ataques a los sistemas
y minimizar la posibilidad de que se produzcan fugas de información utilizando o teniendo activados los "firewalls" y adoptar toda medida adicional de protección que se considere conveniente como por ejemplo el envío de la información cifrada en la que sólo aquella persona que tenga las claves necesarias pueda hacer legible la información contenida en el archivo.

### 6.6.2 Nivel de seguridad

Como se indica en el artículo 3 del Reglamento de Medidas de Seguridad, se establecen atendiendo a la naturaleza de la información tratada y se aplicarán, según se recoge en el artículo 4 (1), de tal forma que han de adoptarse las medidas de seguridad de nivel básico y, para aquellos ficheros que contengan datos especialmente protegidos, deberán adoptarse las correspondientes al nivel alto.

Como los centros privados concertados tratan datos de salud de sus alumnos, las medidas de seguridad que deben implantar los responsables son las de nivel alto. Se hace necesario segregar y calificar que tipo de ficheros requieren medidas de seguridad de tipo alto y cual básicas y aplicarlas conforme a la legislación al respecto.

### 6.6.3 Documento de seguridad

Este aspecto del que casi todos los Centros son deficitarios es de obligada cumplimentación máxime cuando se tratan datos especialmente protegidos y amparados por la ley de manera especial.

(1) **Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999 de 11 de junio de 1999** ***Artículo 3***. Niveles de seguridad. 1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto. 2. Dichos niveles se establecen 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. ***Artículo 4***. Aplicación de los niveles de seguridad. 1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico. 2. 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 artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio. 3. 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 de nivel alto. 4. 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. 5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

Como se hace mención en el CAPÍTULO II sobre el documento de seguridad en el artículo 88 (1) del RD 1720/2007 sobre el documento de seguridad 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.

Además el documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento como es el caso que nos ocupa para poder facilitar un poco el trabajo de los Centros y no tener que aplicar niveles de seguridad alta a todos los ficheros. 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.

Este 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.

**(1)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** CAPÍTULO II Del documento de seguridad ***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.

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.

El Reglamento de Medidas de Seguridad requiere para todo tipo de fichero la existencia de un documento de seguridad. Por tanto, resulta preciso elaborar el mismo, máxime cuando, como ha quedado señalado, se tratan datos especialmente protegidos.
En los casos en que dicho documento ya existe, es preciso hacer operativas todas las medidas de seguridad recogidas en el mismo.

### 6.6.4 Funciones y obligaciones del personal

En este apartado se habla de las obligaciones propias del personal tanto del docente como el de administración y servicios.

Estas funciones y obligaciones deben ser entregadas y firmadas por cada uno de los trabajadores del Centro Escolar asegurando así el conocimiento por parte de todos de sus obligaciones y funciones en función del cargo que regenta en el Centro.

Se debe hacer firmar a los trabajadores un "Acuerdo de Confidencialidad", que sea suscrito por el personal no docente que preste sus servicios en el centro, en el que se indica la prohibición de acceder a "cualquier tipo de información que esté en cualquier tipo de soporte y que se encuentre en cualquiera de los locales".

Como en muchos centros escolares no hay documento de seguridad, resulta preciso incidir en la necesidad de su elaboración ya que, dentro del mismo, deberían aparecer recogidas las funciones y obligaciones del personal.

En los supuestos de que los centros escolares privados concertados dispongan del correspondiente documento de seguridad, en el que se incluyen las funciones y obligaciones

del personal, es requisito imprescindible que las mismas se comuniquen al personal del centro con acceso a datos de carácter personal.

### 6.6.5 Gestión de incidencias

En función de la tipología de los datos tratados así serán las medidas de seguridad exigibles, si son de nivel básico, se debe observar lo dispuesto en el artículo 10 (1) del Reglamento y si estas medidas son de nivel alto, además del citado artículo, se debe atender lo dispuesto en el artículo 21 (2) del Reglamento de Seguridad.

Debe ser establecido un procedimiento de gestión y notificación de incidencias, en los términos establecidos en el Reglamento de Medidas de Seguridad.

Resulta preciso que los centros privados concertados cuenten con un registro de incidencias, en el que quede constancia el procedimiento de notificación y gestión en el que se haga constar el tipo, el momento de su producción, la persona que realiza la notificación, a quién se le notifica y los efectos que se hubieran producido derivados de la misma.

Esta exigencia resulta, aún más urgente y necesaria, si se advierte que los centros escolares privados concertados al igual que los centros públicos tratan datos especialmente protegidos que, por ello, exigen medidas de seguridad de nivel alto.

(1) Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999 de 11 de junio de 1999 *Artículo 10*. Registro de incidencias. El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma. (2) Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999 de 11 de junio de 1999 *Artículo 21* Registro de incidencias. 1. En el registro regulado en el artículo 10 deberán consignarse, además, 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. 2. Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

### 6.6.6 Control de accesos

En este apartado, se comenta lo dispuesto por la normativa de protección de datos, en lo referente a la identificación y autenticación, así como todo lo relativo al acceso a los datos personales y al acceso físico a los mismos.

Este aspecto es de vital importancia debiendo siempre establecer por escrito procedimientos de asignación, distribución y almacenamiento de las claves de identificación y autenticación para acceder a los sistemas de información que tratan los datos personales de los alumnos. Debe, además, existir una relación actualizada de los usuarios que tienen acceso autorizado a dichos sistemas dando de alta o en su caso de baja a los usuarios y otorgando los privilegios propios a su cargo en el Centro escolar.

La mayoría de los centros escolares emplean un código de usuario y contraseña para acceder al sistema de información que gestiona los datos personales de los alumnos.
Estas contraseñas las suele proporcionar el administrador del sistema y suele almacenarse de forma inteligible. Se dan otros casos que tienen una longitud no segura, de cuatro dígitos, o son totalmente adivinables con pocos intentos.
Estos aspectos deben ser tenidos en cuenta en los Centros y mejorados para evitar el uso fraudulento o robo de información que puede ser especialmente protegida.

En ocasiones la contraseña usada para acceder a los datos es compartida por lo que los privilegios de uno son los mismos que los de otros no adecuando su cargo a los derechos que tiene.

El acceso a los locales donde se encuentran ubicados los sistemas de información con datos de carácter personal debe estar reservado a las personas autorizadas y no tenerlos abiertos por comodidad abriendo la posibilidad de robo de datos personales.

Siempre que haya un soporte con datos personales deberemos implementar medidas de seguridad tanto sean soportes informáticos como soporte papel máxime si estos soportes contienen datos especialmente protegidos.

El acceso a los expedientes únicamente debe estar permitido a aquellas personas que disponen de la llave del archivo, o de las salas donde se almacenan no debiendo dejarlos nunca en salas de acceso público.

Los datos han de ser accedidos por aquellos usuarios que los necesiten para su trabajo, para lo cual han de estar justificados los permisos de acceso de cada uno por parte del responsable del fichero.
Se ha de mantener un registro de accesos al sistema, conservándose los mismos al menos dos años, según dispone el artículo 24.4 (1) del Reglamento de Medidas de Seguridad.

Se ha de comprobar que las contraseñas se cambian periódicamente y que se siguen normas para hacerlas seguras como la longitud, el uso de caracteres alfanuméricos.

Se recomienda utilizar protectores de pantalla para evitar el acceso al ordenador por parte de terceros no autorizados.

### 6.6.7 Gestión de soportes

Los centros escolares disponen de soportes informáticos que contienen datos de carácter personal de los alumnos, sin embargo, no existe una legislación específica ni en la Comunidad ni a nivel Nacional en cuanto a procedimientos que permitan su gestión, ni suelen estar inventariados desde el punto de vista de la normativa de protección de datos.

Es por tanto necesario de tener un registro de soportes actualizado en cuanto a su gestión y distribución.

Por otra parte, debemos prestar verdadera atención a aspectos como los profesores de algunos centros escolares privados concertados se suelen llevar a su domicilio particular los exámenes que realizan sus alumnos para corregirlos. Y es que el problema es muy importante porque

(1) **Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999 de 11 de junio de 1999Artículo 24. Registro de accesos.**

4. El período mínimo de conservación de los datos registrados será de dos años

están llevando datos personales de alumnos sin ningún tipo de seguridad con la posibilidad de perder estos soportes con datos personales.

En otras ocasiones, se llevan pen drivers con los listados de sus alumnos para incorporar la nota correspondiente a los exámenes de evaluación. Por tanto se hace necesario dar instrucciones al personal docente de los centros privado-concertados para que sepan cómo proceder y que hacer en el caso de pérdida de información.

En el documento de seguridad que como ya hemos indicado es de obligado cumplimiento y realización se prevé la realización de tratamientos fuera de los locales donde se ubican los ficheros, eso sí con previa autorización del responsable de seguridad y garantizándose el nivel de seguridad correspondiente.

Es por ello que todos los soportes informáticos han de estar inventariados, de manera que sea posible identificar los datos contenidos en ellos. Además se ha de disponer de procedimientos de distribución y reutilización de soportes.
Por lo que se refiere al registro de entrada/salida de soportes, se ha de disponer del mismo en los términos del Reglamento de Medidas de Seguridad.

Respecto a la destrucción de los documentos, se ha de verificar que la misma se produce de modo que se impida el acceso a los mismos por parte de terceros, y, en el caso de usar empresas externas para realizarlo, se ha de haber suscrito un contrato, que recoja los extremos previstos en el artículo 12 de la LOPD, y obtener un certificado de destrucción a tenor de lo pactado.

Cuando se vayan a sacar datos de los alumnos fuera del centro escolar, es preciso que quede constancia de ello en el registro de gestión de soportes y que sea autorizada la salida por el responsable del fichero, que fijará además el modo de hacerlo.

### 6.6.8 Copias de respaldo y recuperación

Como ya se ha indicado en el apartado relativo a copias de respaldo y recuperación en Centros públicos, los centros educativos no dispones de una normativa o recomendaciones de

cómo y cuándo realizar copias de seguridad y respaldo de los ficheros con los que trabajan. Como además no realizan el documento de seguridad no contemplan esta cuestión. Y es que los Centros Escolares deben de realizar al menos una vez a la semana una copia de seguridad y respaldo y también siempre se produzcan modificaciones de los ficheros que contienen datos de carácter personal.

Otro aspecto que debe cuidarse por parte de los Centros Escolares es el medio físico o soporte en el que deben de hacer las copias de seguridad. Estos soportes deben de ser diferentes al medio del que provienen y deben ser totalmente legibles para que pueda ser revisado sin ningún tipo de problema.

Además deberá ser revisado que estas copias de recuperación se encuentren bien custodiadas para que los datos personales no puedan ser robados por terceros.

Por lo tanto, se ha de fijar un procedimiento para la obtención de una copia de respaldo y de recuperación de datos, cumpliendo las medidas previstas en el Reglamento de
Medidas de Seguridad.

Dichas copias se han de custodiar en un lugar diferente a aquel en que se encuentran los equipos informáticos, y se realizarán al menos una vez a la semana, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
Las copias se han de verificar para comprobar que los datos allí almacenados son legibles.

### 6.6.9 Responsable de seguridad

Como se recoge en el artículo 16 del Reglamento de Medidas de Seguridad "*El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento*".

Resulta preciso que el responsable del fichero nombre a un responsable de seguridad, en los términos establecidos en el Reglamento de Medidas de Seguridad advirtiendo al responsable

del tratamiento de los datos personales que el que haya un responsable de seguridad no le exonera de sus obligaciones como máximo responsable del tratamiento de los datos personales de los interesados.

### 6.6.10 Auditoría

El Reglamento de Medidas de Seguridad Real Decreto 994/1999, de 11 de junio, en el artículo 17 recoge todos los aspectos relativos a la Auditoría. En el apartado 1 se contempla lo siguiente:

"*1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoria externa interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años*".

Resulta preciso que se realicen las auditorías de los sistemas de información, de modo que se examine sobre la adecuación de las medidas y controles previstos en el Reglamento de Medidas de Seguridad, así como sobre la identificación de las deficiencias y medidas correctoras o complementarias necesarias. Dicha auditoría quedará a disposición de la Agencia Española de Protección de Datos.

### 6.6.11 Telecomunicaciones

En el artículo 26 del Reglamento de Medidas de Seguridad, se recoge lo relativo a las Telecomunicaciones, y señala que "*La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismos que garantice que la información no sea inteligible ni manipulada por terceros*".

Toda transmisión de datos por redes de telecomunicaciones ha de realizarse con las necesarias medidas de seguridad y debe de efectuarse cifrada o de manera que la información sea ininteligible y no manipulable por terceros. Por ello, en caso de envío de datos por correo electrónico, se ha de verificar que los mismos se transmitan de forma cifrada pudiendo usar una clave privada y clave pública sólo en poder de los interesados.

### 6.6.12 Deber de secreto

El artículo 10 de la LOPD establece que el responsable de ficheros con datos de carácter personal, así como todas aquellas personas que intervengan en el tratamiento de datos de carácter personal, están obligados al secreto profesional, aspecto que deben de tener en cuenta tanto los Centros Públicos como Privados-Concertados.

En su función educativa son muchos los profesionales como profesores y la colaboración de distintos profesionales como pueden ser psicólogos, pedagogos, médicos, personal administrativo y de limpieza. Todos ellos, en algún momento, acceden o pueden tener acceso a los sistemas de información o documentación que contienen datos personales de los alumnos.

En la LOE en su disposición adicional vigésimo tercera, apartado 3, establece lo siguiente:
"*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*".

Como ya hemos indicado en la ORDEN EDU/1951/2007, de 29 de noviembre en la Disposición adicional Primera (1), el tratamiento de los datos personales del alumnado se ajustará a lo dispuesto en la disposición adicional vigésima tercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos y en sus normas de desarrollo por lo que deberemos de ceñirnos a las leyes antes mencionadas.
Por tanto, se estima oportuno que se remita, a todo el personal que presta servicios en los centros privados concertados, una instrucción en la que se recuerde el deber de sigilo que impone el artículo 10 de la LOPD y la disposición adicional vigésimo tercera de la LOE.

(1) **ORDEN EDU/1951/2007, de 29 de noviembre *DISPOSICIONES ADICIONALES Primera***.– Datos personales del alumno. El tratamiento de los datos personales del alumnado se ajustará a lo dispuesto en la disposición adicional vigésima tercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos y en sus normas de desarrollo.

### 6.6.13 Cesiones de datos

En los Centros Educativos tanto públicos como Privado-Concertados existen bastantes cesiones de datos que vamos a ir analizando.

El artículo 11 de la LOPD, en su apartado 1, recoge lo siguiente:
"*1. 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*".

Los centros privados concertados están obligados a ceder los datos personales de los alumnos/as a la Administración para la realización de determinados trámites impuestos por la legislación educativa por lo que hay habilitación legal de estas cesiones amparadas por la Ley orgánica 2/2006, de 3 de mayo, de Educación en su disposición adicional vigésimo tercera en los apartados 1 y 4 en los que se indica:

"*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.*

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*."

Además, como se indica en el artículo 117 (1) de la LOE 2/2006 de 3 de mayo en el apartado 5 los salarios del personal docente serán abonados por la Administración al profesorado como pago delegado y en nombre de la entidad titular del centro, con cargo y a cuenta de las cantidades previstas en el apartado anterior. A tal fin, el titular del centro, en su condición de empleador en la relación laboral, facilitará a la Administración las nóminas correspondientes, así como sus eventuales modificaciones.

En otros casos, es posible que no haya la habilitación legal para realizar estas cesiones a la Administración y se dan datos personales sin conocer el centro privado concertado que dicha cesión cuente con justificación legal razón por la cual nos debemos asegurar que hay habilitación legal para estas cesiones.

Por otra parte, los centros privados concertados suelen ceder datos personales a empresas privadas.
Dentro de las cesiones sean o no legales a la Administración destacamos:

**Comisión de Escolarización:**

Los colegios suelen remitir una copia de las solicitudes de plaza que se han presentado en el colegio, baremadas, correspondientes a los alumnos que no han sido admitidos, para que se les asigne plaza escolar en otro centro.

**Consejería de Educación:**

Datos de los alumnos para que se expida el libro de escolaridad (nombre y apellidos, fecha de nacimiento, localidad, provincia, país de nacimiento y nacionalidad).
Relación de alumnos admitidos en el colegio y, en otros casos, la relación que se remite contiene los datos personales de los alumnos matriculados.
Una vez que los alumnos finalizan la enseñanza básica, el centro ha de solicitar el título correspondiente para cada alumno y este trámite se suele realizar ante la Consejería de Educación, previa remisión de los datos personales de los alumnos, según el modelo

**(1) Ley Orgánica 2/2006 de 3 mayo de Educación** ***Artículo117 apartado 5***. Los salarios del personal docente serán abonados por la Administración al profesorado como pago delegado y en nombre de la entidad titular del centro, con cargo y a cuenta de las cantidades previstas en el apartado anterior. A tal fin, el titular del centro, en su condición de empleador en la relación laboral, facilitará a la Administración las nóminas correspondientes, así como sus eventuales modificaciones.

establecido por cada una. En algunas Comunidades Autónomas este listado se entrega en el Instituto de Educación Secundaria al que se encuentra adscrito el colegio.

Los centros privados concertados actúan como intermediarios, entre las familias y la Consejería de Educación de la Comunidad Autónoma o en algunos casos con la Administración Central en el proceso de solicitud de becas.
Remiten los formularios cumplimentados y añaden información certificando la reserva de plaza. Acompañan a los formularios una relación de becas solicitadas.

También, la inspección educativa en el ejercicio de sus funciones puede accede a los expedientes, que custodia el departamento de orientación del colegio, para verificar la adecuación de las necesidades educativas de un alumno concreto, con los estudios y evaluaciones realizadas por los profesionales del centro.

Se suele entregar además, a la inspección educativa una relación nominal de alumnos, clasificados según los siguientes criterios: necesidades educativas especiales, minorías éticas y minorías socioculturales.

Algunos centros privados concertados remiten al Servicio de Inspección de Educación el documento de organización del centro, conteniendo relaciones nominales de alumnos con necesidades educativas especiales.

Los dictámenes elaborados por el orientador de algún colegio, sobre alumnos que necesitan adaptación curricular, se remiten al Equipo Especializado de Orientación Educativa y Psicopedagógico de la Consejería.

Cuando un alumno necesita ser evaluado por el Equipo Especializado de Orientación Educativa y Psicopedagógico de la Consejería de la Consejería de Educación y, previa autorización de la Dirección General de Orientación Educativa, el centro remite al citado equipo un informe psicopedagógico realizado por el departamento de orientación, que puede contener diagnósticos médicos.
Se remite, para su aprobación, el Dictamen de Escolarización que elabora el departamento de orientación del centro sobre los alumnos con necesidades educativas especiales.

Algunas de las cesiones citadas, que realizan los centros privados concertados a la Consejería de Educación, vienen amparadas por la legislación que regula el derecho a la educación (por ejemplo para la obtención del libro de escolaridad, para la emisión de los títulos, y para la gestión de las pruebas de acceso a la universidad).

**Consejería de Sanidad:**

Se suele dar una relación de alumnos que van a formar parte de las campañas de salud que organiza la Consejería o de datos de vacunación o similares.

**Universidad:**

Se suelen entregar dos tipos de listados, uno inicial, con nombre y apellidos, de todos los alumnos matriculados en segundo curso de Bachillerato que, posteriormente, suele actualizarse con los datos personales de aquellos alumnos aprobados que van a presentarse a las pruebas de acceso a la universidad.

**Tesorería General de la Seguridad Social:**

Se comunican los datos de los alumnos que cursan estudios a partir de tercero de la ESO, al objeto de tramitar la solicitud del seguro escolar.

**Otras cesiones:**

Cuando se detectan ausencias injustificadas y continuas de un alumno que cursa alguna enseñanza básica, se comunican sus datos a los Servicios Sociales del Ayuntamiento o de la Consejería de Educación para que entre en contacto con la familia recordándole la obligatoriedad de permanecer escolarizado.

Cuando un alumno se incorpora a otro centro escolar sin finalizar el ciclo, el colegio remite al de destino el libro de escolaridad, expediente académico, informes médicos y los informe psicopedagógicos así como, en algún caso, las pruebas psicotécnicas.

Los centros escolares ceden datos personales de sus alumnos a las entidades aseguradoras con las que han suscrito alguna póliza de seguros, en aquellos casos en los que se produce algún siniestro. En este caso se suele utilizar un formulario elaborado por la entidad aseguradora.

Algún colegio entrega datos personales de los alumnos que finalizan los estudios a su Asociación de Antiguos Alumnos.

En los colegios privados concertados donde existe la AMPA, suele entregarse un listado completo de padres o tutores, sobre todo en aquellos casos en los cuales la pertenencia a la citada asociación es obligatoria.

Algún colegio entrega a los padres o tutores una relación completa de los compañeros de clase de su hijo/a con datos entre los que se encuentran el nombre y apellidos, nivel y aula, domicilio, cuando no debe hacerse bajo ningún concepto a no ser que haya una cesión de datos expresamente autorizada por los interesados.

Fuera de los casos que cuentan con habilitación legal, los centros privados concertados han de contar con el consentimiento de padres o tutores, o, en su caso, si son mayores de 14 años de los propios alumnos.

Por tanto, las cesiones mencionadas, como es la entrega de datos a la AMPA, a asociaciones de antiguos alumnos, etc.…, deben de disponer del consentimiento exigido por la normativa de protección de datos, aspecto que especialmente debe ser cuidado para no incumplir con la LOPD.

### 6.6.14 Prestaciones de servicios

Los centros escolares privados concertados, en algunas ocasiones, necesitan acudir a terceras empresas o profesionales para que les presten determinados servicios.
El artículo 12 de la LOPD "Acceso a los datos por cuenta de terceros", indica lo siguiente:

"*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*."

Los centros privados concertados acuden a terceras empresas para que les presten uno o varios servicios, en las siguientes ocasiones:

- Centros que acuden a asociaciones que les facilitan profesionales especializados para atender a niños con necesidades educativas especiales.
- Centros que utilizan servicios de empresas que gestionan el servicio de comedor o escuelas de música. Las empresas suelen elaborar un formulario de recogida de datos, que el centro entrega a los padres para que lo cumplimenten, y que posteriormente entrega a la empresa.
- Las empresas o agrupaciones deportivas que gestionan e imparten las actividades deportivas o extraescolares.
- 
- Empresas a las que acuden los alumnos de formación profesional para realizar prácticas laborales.

- Empresas que gestionan el transporte de los alumnos, a las cuales se les entrega un listado con el nombre y apellidos de los alumnos que van a utilizar este servicio.
- Colegios que han contratado los servicios de tratamiento de datos personales con una empresa externa.
- Los gabinetes fotográficos, que elaboran la orla, tienen conocimiento del nombre y apellido de cada uno de los alumnos a los que fotografían, sobre todo en 2º de Bachiller o cursos finales de etapa educativa como 3º Infantil, 6º de Primaria o 4º de la ESO.
- Empresas que elaboran las revistas o anuarios del colegio, donde se incluyen fotografías y datos personales de los alumnos.
- Algunos colegios han contratado los servicios de una empresa para alojar su página "Web".
- Empresas encargadas del mantenimiento de la aplicación utilizada por los colegios para la gestión de los datos personales de sus alumnos.
- Empresas a las que los colegios privados concertados encargan el mantenimiento de sus sistemas informáticos, que son utilizados para gestionar los datos personales de sus alumnos.

El colegio realiza las comunicaciones a los padres por encargo de la AMPA.
El AMPA, en algunos colegios, ha suscrito una póliza con una aseguradora, a la que facilita los datos identificativos de todos los alumnos que cubre la póliza.
Algunos colegios cuentan con los servicios de un psicólogo, que es el encargado de atender a aquellos alumnos que lo necesitan, o de realizar pruebas psicotécnicas a todos los alumnos del colegio.

En los contratos de prestación de servicios, en los que el contratista accede al tratamiento de datos por cuenta del responsable del fichero, resulta necesario que el contrato se formalice por escrito y que recoja los extremos a que se refiere el artículo 12.2 y 3 de la LOPD.

Por ello se recomienda la revisión de todos los contratos para que, si no encuentran habilitación en el artículo 11 de la LOPD, adecuen su forma y contenido al citado artículo 12.

### 6.6.15 Transferencias internacionales de datos

Como se indica en el artículo 33:

"*1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.*

*2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países*."

Cuando la comunicación de datos se efectúa a un país fuera de los que forman parte del Espacio Económico Europeo, es preciso que el Director de la Agencia Española de Protección de Datos autorice dicha transferencia internacional de datos. Por el contrario, cuando no sea así, la comunicación puede realizarse, teniendo presente la necesidad de formalizar la relación jurídica a través de un contrato que reúna las condiciones previstas en el artículo 12 de la LOPD.

Por tanto, se recomienda que, a tenor de lo previsto en el artículo 33 de la LOPD, se revisen las comunicaciones que se puedan efectuar entre centros escolares de distintos países como en algunas ocasiones en intercambios de alumnos.

## 7. Comercio electrónico en los Centros educativos

- **Generalidades**
- **El Comercio electrónico en la normativa española**
- **Nombres de dominio**

## Comercio electrónico en los Centros educativos

### 7.1 Generalidades

El comercio electrónico, en palabras sencillas, es cualquier transacción operativa realizada vía proceso digital o redes de trabajo.
Sin embargo, el comercio electrónico es algo más que el simple mercado de productos o servicios vía Internet.
El comercio electrónico es:

- Una tecnología promocional que permite a las empresas incrementar la precisión y la efectividad en la transacción de sus transacciones comerciales y
- Una forma de intercambio de información entre organismos, clientes y comerciales para el beneficio de todos.

El comercio electrónico se está desarrollando a un ritmo rápido. Muchos organismos y personas individuales buscan en el mundo de la Web el futuro, una fuente segura de información, materias, servicios y comunicación.

Hoy día las actividades empresariales que se llevan a cabo en la Web están aumentando, la cantidad de mercancías, servicios e información que se intercambia en Internet parece que va a ser doblado o triplicado. Es muy común en el entorno de organismos pequeños y grandes, privados o administraciones públicas, que se vean forzados a desarrollar actividades en la Web tanto los clientes como los competidores.

En algunos casos incluso las empresas tradicionales pierden su acceso al juego del comercio electrónico, ya que no quieren perder sus clientes. Según todas las pistas el comercio

electrónico se continuará desarrollando y, consecuentemente, muchos organismos se verán forzados, a utilizar Internet como una vía, o a cerrar.

El comercio electrónico cambia la forma en que los productos, los servicios, incluso la información que es presentada, vendida e intercambiada, cambian incluso la forma en que los organismos colaboran con los clientes y sus colaboradores.

Finalmente, es común que el comercio electrónico sustituya el intercambio de información impresa dentro y entre organismos, así como entre organismos y clientes.
El comercio electrónico vía Internet se infiltra en nuevos mercados, descubre o crea nuevos canales de ventas o se acerca a los clientes y colaboradores a través de nuevos canales de comunicación. Algunos de los pioneros consiguen importantes resultados, más o menos, el tamaño de las empresas no juega un papel importante, ya que todos los organismos tienen las mismas oportunidades puesto que tienen acceso a Internet.

**Tipos de Comercio Electrónico**

Las empresas, organizaciones públicas y clientes pueden participar en el entorno del comercio electrónico. Las aplicaciones del comercio electrónico pueden ser clasificadas en cuatro categorías:

- Comercio electrónico de la Empresas a los Clientes (B2C).
- Comercio electrónico de los Clientes/Ciudadanos a las Instituciones Gubernamentales (C2G).
- Comercio electrónico de las Empresas a las Instituciones Gubernamentales.
- Comercio electrónico de las Empresas a las Empresas (B2B).

1. **Comercio Electrónico de las Empresas a los Clientes (B2C)**

Las aplicaciones B2C están dirigidas al consumidor medio. Este tipo de aplicaciones de comercio electrónico han sido desarrolladas durante los últimos años, principalmente como resultado del extendido uso de Internet y de la mejora de los servicios provistos por este medio. Internet es aplicable a este tipo de comercio electrónico, ya que es ampliamente

disponible y puede promover productos efectivos y servicios entre todo tipo de posibles clientes.

2. **Comercio electrónico de los Clientes/Ciudadanos a las Instituciones Gubernamentales (C2G).**

Las aplicaciones C2G incluyen en su mayoría pago de impuestos, publicaciones de documentos oficiales, etc. A pesar de que no podemos definir las transacciones entre los clientes o ciudadanos con las instituciones gubernamentales como comercio electrónico, podemos ver suficientes aplicaciones C2G en el marco de transacciones que son realizadas más efectivamente y más eficientemente con el uso de sistemas de tecnología de comercio electrónico.

1. **Comercio electrónico de las Empresas a las Instituciones Gubernamentales.**

Las aplicaciones B2G incluyen los impuestos, los suministros, y el control de aduanas para las importaciones y exportaciones, etc. Como en el caso de las aplicaciones de comercio electrónico entre consumidores e instituciones gubernamentales, las transacciones de las empresas a las instituciones gubernamentales no parecen tener una relación directa con lo que el mundo considera comercio electrónico. Sin embargo, el Estado está relacionado en casi todo tipo de transacción empresarial durante todo el ciclo comercial y por esta razón bastantes aplicaciones han sido desarrolladas con el fin de mejorar las transacciones B2G.

2. **Comercio electrónico de las Empresas a las Empresas (B2B).**

Las aplicaciones B2B tienen como objetivo la mejora y simplificación de varios procesos operativos en las empresas, así como el incremento de la eficiencia de las transacciones entre empresas colaboradoras.

Las empresas utilizan el sistema B2B para transacciones más rápidas sin faltas, para control de reservas, sustitución efectiva de productos, etc. Las empresas que desarrollan actividades B2B para comercio electrónico con sus colaboradores deben tener colaboración y coordinación. Una aplicación B2B implica normalmente a muchas personas individuales en muchas operaciones corporativas. Incluso si la mayor parte de la gente conoce ya las

aplicaciones electrónicas de Empresas a consumidores y un gran número de Empresas pasa del comercio tradicional a los sistemas electrónicos de venta, la transacción más importante del comercio electrónico llevada a cabo es la del tipo B2B. Esto ocurre porque las aplicaciones B2B incluyen millones de transacciones, inversiones tremendas, así como la velocidad y la precisión pueden ser una gran ventaja competitiva.

**Ventajas y desventajas**

**Ventajas del Comercio electrónico para el consumidor**

- Las tiendas electrónicas están abiertas 24 horas al día. En otras palabras, cuando quieras puedes comprar un CD, un billete de avión, o incluso diferentes materiales para la construcción.
- El coste de los productos vendidos a través de Internet es generalmente bastante menor que los precios que se pueden encontrar en el mercado, ya que una tienda electrónica es libre de costes que una tienda real debe soportar (alquiler, electricidad, agua, etc.) y generalmente requiere menos personal.
- El comercio electrónico se está extendiendo globalmente. En otras palabras, a través del ordenador puedes comprar algo que no puedes encontrar en España, de otra manera tendrías que esperar a que algún amigo viajase y te lo trajese.
- La transacción es rápida y directa. Puedes recibir el producto que has pedido en 3-4 días.
- Cualquiera puede encontrar lo que quiere, no importa lo que quiera, sin perder tiempo y desde donde quiera.

**Ventajas del comercio electrónico para la empresa**

- Como hemos mencionado antes, cada empresa que tenga presencia electrónica puede extender sus fronteras extendiendo los límites geográficos de sus transacciones. Esto significa que cada empresa puede tener clientes en varias regiones y países de todo el mundo. En otras palabras, con el comercio electrónico las empresas adquieren varias marcas y lo más importante es que minimizan sus costes.
- Cada empresa que utiliza las nuevas tecnologías –como Internet- se hace más competitiva, y puede ser informada de los nuevos desarrollos. En otras palabras, en

pocos años todas las actividades comerciales se realizarán vía Internet, el comercio electrónico será el nuevo gran desafío para todas las empresas que quieran ser competitivas.

- Las transacciones electrónicas permiten una relación bidireccional entre empresa y cliente (interacción). Esto significa que cada empresa a través de las transacciones electrónicas puede recolectar mucha información sobre las necesidades de los consumidores, según cómo la empresa ajuste su política será más beneficiosa.
- Conociendo las necesidades particulares de los clientes, las empresas pueden avanzar en la creación de productos concretos para un consumidor o grupo de consumidores que necesitan un nuevo producto que todavía no existe en el mercado.

**Desventajas del comercio electrónico**

1. Falta de seguridad, estandarización, fiabilidad

Habitualmente la seguridad y fiabilidad son difíciles de asegurar en Internet. Por otro lado, el mundo confía en la red cuando puede ser comprobada y fiable. Por ejemplo, utilizamos la red de Instrumentos de Transacciones Automáticas es decir los bancos, y confiamos en ellos nuestras transacciones diarias.

2. Insuficiente amplitud de área de comunicación

La red se enfrenta a serios problemas de circulación y falta de suficiencia en el transporte de datos debido al rápido crecimiento de usuarios conectados. La red de tecnologías se desarrolla rápidamente, pero la necesidad de mayor amplitud de área y consecuentemente de velocidad en el transporte de datos, está incrementando debido a un ritmo todavía muy lento, y hasta que se le haga frente, los problemas referidos a la calidad de los servicios continuarán.

3. Dificultad de incorporación de tecnologías de comercio electrónico en los sistemas actuales de gestión de la información.

Muchas empresas utilizan sistemas de información, que ya existían y que fueron desarrollados con el fin de servir a las diferentes necesidades utilizando diferentes tipos de software y aplicaciones. Estos sistemas contienen informaciones precisas para la empresa, pero deberían armonizarse con las nuevas tecnologías, que en muchos casos es excepcionalmente difícil.

4. No todos los clientes tienen acceso a Internet.

En muchos países, como Japón o USA, el porcentaje de usuarios de Internet es bastante elevado. Sin embargo, en la mayoría de los demás países (incluso en los países de Europa Este) el porcentaje de usuarios de Internet es mucho menor. Si el mundo no tiene acceso a Internet, el esfuerzo no alcanza al consumidor.

Naturalmente, se espera que esto cambie en breve, ya que el número de usuarios está aumentando considerablemente.

5. Se requieren gastos de infraestructuras

Incluso si las empresas reconocen la importancia del comercio electrónico en el moderno entorno empresarial, las inversiones en infraestructuras son un factor que debería apreciarse y tomarse en seria consideración.

6. Mucha gente se resiste a cambiar y no están acostumbrados a las transacciones impersonales sin la existencia de documentos.

## Modelos básicos de comercio electrónico

Los modelos básicos empresariales y tecnológicos del comercio electrónico para la integración operacional y corporativa incluyen lo siguiente:

### Tiendas electrónicas

Inicialmente fueron creadas con el fin de presentar la empresa y sus productos. En etapas posteriores las tiendas electrónicas ofrecieron la posibilidad de pedido y pago.

Los beneficios de la empresa incluyen el incremento de demanda, la presencia mundial con bajo coste, la reducción de los gastos de promoción y ventas. Los beneficios para el consumidor son los precios más bajos, más oportunidades, mejor información, comodidad en la elección y el pedido, y distribución de los productos a la casa o a la oficina del cliente. Después de visitas regulares es también posible la promoción de productos independientemente.

### Abastecimiento electrónico

La oferta y abastecimiento electrónico de mercancías y servicios es un servicio útil para las grandes empresas y las Autoridades Públicas. Sus beneficios incluyen más posibilidad de elección de mercancías (y a más bajo coste), mejor calidad, mejora en la forma de entrega, y

disminución en los costes de comisión. Los beneficios para los abastecedores son la mayor oportunidad de propuesta de ofertas (a escala mundial), así como los costes más bajos de propuesta de oferta.

**Subasta electrónica**

La subasta electrónica es la forma vía Internet de subastas. El proceso se realiza vía Internet, los contactos, el pago y la entrega. Los beneficios para los abastecedores y los compradores han incrementado el rendimiento y ahorro de tiempo, la presencia física no es necesaria, contactos con el mundo entero.

**Centros Comerciales Electrónicos**

El Centro Comercial Electrónico es un conjunto de tiendas electrónicas, donde se aplica un método común de pago y todas las tiendas están bajo un "paraguas" (nombre) común. Los beneficios para los miembros de un centro comercial electrónico son los bajos costes y los procesos de importación menos complicados en la Web mundial, las especiales posibilidades (por ejemplo, pagos electrónicos), más tráfico.

Las ventajas de los clientes son el fácil acceso a otras tiendas electrónicas, el medio común de uso (así como servicios adicionales de valor añadido).
Además, los beneficios para el administrador del centro comercial electrónico son los espacios de anuncios, la promoción de marcas, el incremento de ventas de tecnologías de apoyo (ej. IBM con el World Avenue), beneficios resultantes de servicios (ej. Barclays con Barclay Square).
Los ingresos incluyen subscripción de miembros, publicidad y también cuotas de transacciones.

**Comunidades Virtuales**

El valor absoluto de las "comunidades virtuales" proviene de sus miembros (clientes y colaboradores) que añaden su información en el entorno básico de comunicación provista por el servicio. Las "comunidades virtuales" son importantes para la proyección y la promoción

de productos y servicios, fortalecimiento de la fidelidad de los clientes y por ello, animan a los clientes a expresar sus opiniones.

El beneficio viene de las subscripciones de miembros y de la publicidad. Esto constituye un valor añadido para la promoción de los servicios ya existentes, as í como para la creación de nuevos servicios. Ejemplos: Amazon.com, Apparelex.com, Indconnect.com/steel/web

**Servicios de Abastecimiento**

Están especializados en una operación concreta de la cadena de producción de la empresa (cadena VALOR), ej. Pagos electrónicos, asuntos administrativos, con el fin de convertirlo en ventaja.
Ejemplos: FedEx, UPS

**Explotación de Información y otros servicios**

Estos servicios añaden valor al enorme volumen de datos que se vende en las redes de trabajo abiertas. A menudo se trata de actividades empresariales, tales como búsqueda de información (ej. Yahoo), creación de perfiles de clientes, ocasiones empresariales en el mercado, consejos de inversión, etc.

**Pedidos en tercera persona**

Modelo válido para aquellas empresas que deseen asignar su presencia empresarial en Internet a una tercera institución (como una forma adicional de comunicación y acción empresarial). En los “mercados en tercera persona” se añaden nuevas posibilidades, como la creación de “nombre distintivo” (marca), los pagos, los asuntos administrativos, los pedidos y una completa gama de transacciones seguras. Este modelo interesa principalmente a los bancos y proveedores de servicios de Internet (ISP). El beneficio viene de la subscripción de los miembros, los pagos de servicios y transacciones o los porcentajes en el valor de las transacciones.
Ejemplos: Citius, Trade Zone, FedEx.

**Plataformas de Colaboración**

Proporcionan una herramienta total y un entorno de información y colaboración entre empresas. Se centran en operaciones concretas. Las oportunidades empresariales vienen de la gestión de la plataforma (subscripciones/pagos de uso) y la venta de herramientas especializadas (planning, flujo de trabajo, gestión de documentos).

## 7.2 El Comercio electrónico en la normativa española

La Ley 34/2002 de 11 de julio de Servicios de Sociedad de la Información de Comercio Electrónico o como comúnmente se denomina Ley de Comercio Electrónico (LCE) consta de 45 artículos distribuidos en seis Títulos.

Dentro de esta Ley debemos conceptualizar que es un Servicio de la Sociedad de la Información y que es un prestador de éstos.
Un servicio de Sociedad de la Información es todo servicio prestado generalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

Por otra parte, un prestador de servicios de sociedad de la Información es toda persona física o jurídica que proporciona un servicio de la sociedad de la información. La prestación de servicios de la Información se rige por el principio de libre prestación, lo que implica que no es necesaria ninguna autorización previa para poder prestar servicios de sociedad de la información en el ámbito de la denominada sociedad de la Información, eso sí, sin perjuicio de los regímenes de autorización previstos en el ordenamiento jurídico.

Se entiende que un prestador de servicios está ubicado en España cuando su residencia o domicilio social se encuentran en territorio español siempre que éstos coincidan con el lugar en que efectivamente esté centralizada la gestión administrativa y la dirección de los negocios.

La ley 34/2002 será de aplicación a los servicios de la sociedad de la Información que se ofrezcan en territorio español de manera permanente, es decir, cuando alguna de las sucursales se haya inscrito en el Registro Mercantil o en otro Registro público español en el

que fuera necesario la inscripción para la adquisición de personalidad jurídica. Todos los prestadores de servicios de la Información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que le sean de aplicación, en función de la actividad/es que desarrollen, con independencia de la utilización de medios electrónicos para su realización.

Y es que Internet es una red social que el Derecho no puede desconocer y debido a la gran demanda y universalización de Internet hay que acotar y desarrollar una normativa que ponga coto y unas líneas claras de actuación para todos.

Con la aprobación de esta Ley se incorpora a nuestros ordenamientos jurídicos a la Directiva 2000/31/CE del Parlamento Europeo y de Consejo del 8 de junio. Se vienen a regular aspectos como las comunicaciones comerciales, la presencia de una empresa en Internet, las relaciones comerciales y los contratos electrónicos entre estas y los consumidores. Con el marco jurídico presentado se proporciona la confianza necesaria para emplear las redes de telecomunicaciones y en especial la de Internet, de manera que se aprovechen sus innumerables ventajas por parte de los usuarios como ya hemos indicado anteriormente.

Esta Ley favorece la celebración de Contratos Electrónicos al reconocerse la plena validez y eficacia jurídica del consentimiento prestado por vía electrónica, fijando el lugar y el momento donde se presumirá celebrado el contrato. Se fomenta también la elaboración de códigos de conducta que son los instrumentos de autorregulación especialmente aptos para adaptar los diversos preceptos de la Ley y a las características específicas de cada sector.

En relación a las obligaciones de los prestadores de servicios de la sociedad de la información se contemplan la de dejar constancia registral de su nombre de dominio, proporcionar a los destinatarios del servicio acceso electrónico a la información requerida por la Ley, bastando con su inclusión en su sitio de Internet, el deber de colaboración de los prestadores de servicios de intermediación cuando un órgano competente lo requiera, retener los datos de tráfico relativo a las comunicaciones electrónicas por un periodo máximo de doce meses y el deber de colaborar con el Ministerio de Ciencia y Tecnología y con los demás órganos competentes en la materia.

Dentro de este marco podemos añadir un nuevo elemento que es el de prestadores de servicios de intermediación que también están sometidos a la LCE como podemos tener constancia en el artículo 1.1 (1) de la misma. Según la LCE podemos distinguir 4 tipos de servicios de intermediación:

- Operadores de redes y servicios de telecomunicaciones electrónicas que básicamente transmiten los datos facilitados por el destinatario o en facilitar o en facilitar acceso a las redes de telecomunicaciones.
- Prestadores de servicios de intermediación que transmiten por una red de telecomunicaciones datos facilitados por el destinatario del servicio y que además almacenan en sus sistemas de forma automática, provisional y temporal con la finalidad de hacer más eficaz la transmisión.
- Aquellos prestadores que alojan o almacenan datos proporcionados por el destinatario del servicio.
- Los que facilitan enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos.

El régimen de responsabilidad al que se someten los prestadores de servicios de la sociedad de la información (civil, penal y administrativa) será la establecida con carácter general en el ordenamiento jurídico atendiendo las diferentes funciones que realizan en calidad de prestadores de estos servicios de sociedad de la información.

Además, se contempla el impulso específico que las Administraciones Públicas deben de dar a la elaboración de códigos de conducta, fomentando éstas su elaboración en el ámbito comunitario o internacional.

**(1) La Ley 34/2002 de 11 de julio de Servicios de Sociedad de la Información de Comercio Electrónico** TÍTULO I Disposiciones generales CAPÍTULO I Objeto ***Artículo 1***. Objeto. 1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

En cuanto a la contratación electrónica, se van a producir todos los efectos previstos por el Ordenamiento jurídico cuando converjan el consentimiento y los requisitos necesarios para la formalización de la contratación electrónica. Se excluye de estas disposiciones de la contratación electrónica a aquellos contratos relativos al Derecho de Familia y sucesiones.

La prueba en los contratos electrónicos no presenta ninguna especialidad ya que la validez de éstos es la misma que los contratos realizados por medios tradicionales, y en su caso, la normativa prevista a firma electrónica es la que da veracidad a la contratación electrónica.

Las obligaciones propias de los prestadores de servicios son las propias de las etapas precontractuales y las pos contractuales del Ordenamiento jurídico. En las fases contractuales, la Ley con el fin de esclarecer incógnitas propias de esta etapa, determina que cuando en el contrato interviene un consumidor la realización del mismo será la residencia del mismo y en el caso de contratos electrónicos entre empresas se establece la celebración del mismo el establecido por el prestador de servicios.

En cuanto a las sanciones se diferencian entre muy graves, graves y leves. El incumplimiento de las órdenes provenientes de un órgano administrativo competente en la materia, incumplir la obligación de retener datos de tráfico de las comunicaciones establecidas o utilización de estos para fines distintos de los permitidos constituyen una sanción muy rave que conlleva multas de hasta 600000 €. El envío masivo de comunicaciones comerciales sin solicitud previa o sin consentimiento del mismo, incumplir la obligación de confirmar la recepción de una aceptación o resistirse a la inspección de los órganos facultados al efecto conlleva sanciones con importes de hasta 150000 €. La no inscripción del nombre de dominio o dirección de Internet, faltar al deber de información o no confirmar la aceptación son consideradas faltas leves que son multadas hasta con 30000 €. Las sanciones muy graves serán impuestas por parte del Ministerio de Ciencia y Tecnología las graves y leves las impondrá el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

## 8. Comercio electrónico y contratación electrónica

Por comercio electrónico podemos entender a la compra de productos o servicios por Internet, en un sentido más amplio podemos entenderlo como toda operación comercial utilizando para llevarla a cabo herramientas electrónicas de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial o en el resultado de la actividad que se está desarrollando.

Por contratación electrónica se entiende a aquella contratación que se realiza mediante utilización de algún elemento electrónico cuando éste tiene o puede tener incidencia real y directa sobre la formación de la voluntariedad o el desarrollo o interpretación futura del acuerdo. Una empresa está realizando una actividad de comercio electrónico cuando contempla la utilización de estos medios como canal de comercialización de su oferta, de productos o servicios habiendo adaptado esta oferta a las características de la utilización de la electrónica y la red. En todo comercio electrónico debe de existir un canal de distribución electrónica que en algunos casos deberá completarse con los canales tradicionales de distribución para poder hacer llegar el producto o servicio al cliente o empresa.

Los prestadores de servicios pueden estar presentes de distintas formas en Internet distinguiendo estas formas en función de los objetivos y resultados finales de la presencia en Internet:

- Presencia estática: aquellos prestadores que tengan o puedan tener alguna influencia en la consecución del fin comercial aunque eso sí, no se alcanza ningún tipo de interrelación con el destinatario.
- Presencia dinámica: tenemos dos tipos de presencia dinámica, la que es conversacional, es decir, no existe contratación electrónica, sólo la dinámica de pregunta y respuesta entre ambas partes; por otra parte la presencia dinámica contractual con contratación electrónica en la que se puede llegar a efectuar una contratación vía electrónica bien sea de un producto o de servicios.

Podemos hablar también de las obligaciones derivadas por una parte de la mera presencia en Internet y de los que además ofrecen una contratación electrónica a través de su página Web.

Sólo por una mera presencia en Internet se debe cumplir una serie de obligaciones que detallamos a continuación:

- Comunicación del nombre/s de dominio de Internet que le corresponden al Registro Público en el que conste inscrito para la adquisición de personalidad jurídica o a los sólo efectos de publicidad con el fin de garantizar a los ciudadanos y la Administración Púbica su vinculación a un establecimiento físico y localización o establecimiento en Internet.
- Proporcionar información de manera permanente, fácil, directa y gratuita sobre el nombre o denominación social, residencia, domicilio o dirección de uno de los establecimientos en España, dirección de correo electrónico, datos que permitan comunicación directa y efectiva, datos de inscripción del nombre de dominio en el Registro correspondiente, si está sometido a autorización administrativa, si ejerce profesión regulada indicando nº de colegio y lugar de expedición, precio del producto o servicio y si lleva o no IVA incluido y gastos de envío, si está o no adherido a códigos de conducta y el número de identificación fiscal.
- Facilitar al Ministerio de Industria, turismo y comercio los datos necesarios para que puedan ejercer su función.
- Identificar con la palabra PUBLICIDAD a los correos electrónicos en los que se envíe correo masivo recabando además el consentimiento previo para el envío de las mismas.

Además, todos los prestadores de servicios de la sociedad de la información si realizan contratación electrónica a través de la Web deberán además de las señaladas obligaciones cumplir con la que se detallan a continuación:

- Obligaciones precontractuales: Los distintos trámites para celebrar el contrato; si se va a archivar el documento electrónico que se realice y si es a su vez accesible; los medios técnicos que se ponen a disposición para identificar y corregir errores en la introducción de datos y la lengua/s en que se podrá formalizar el contrato. Tener en cuenta que estas obligaciones siempre serán necesarias cuando haya un consumidor, es decir, no una empresa. Las ofertas o promociones por vía electrónica serán válidas durante el periodo que anuncie el anunciante.

- Pos contractuales: un acuse de recibo por correo electrónico u otro medio electrónico en un plazo de 24 horas tras la recepción de la aceptación como confirmación de la contratación realizada; para la confirmación de la contratación realizada uso de un medio similar al utilizado en la contratación; se considera recibida la confirmación cunado ambas partes tengan constancia del mismo; si se estipula que no es necesaria la confirmación o si ambas partes no son consumidores no será la conformación de aceptación del contrato.

## 9. Nombres de dominio

Al nacer Internet surgió la necesidad de identificar a los ordenadores para poder conocer el origen y destino de la información transmitida por la red. Así surgió la creación de dirección IP que identificaban al origen y al destinatario de los datos que se transmitían. Tras la denominación IP surgió el sistema DNS que daba nombre a las direcciones IP compuestas de número, es decir, hacía de traductor de números a letras haciendo comprensibles las direcciones IP. Estas direcciones IP traducidas en nombres son los nombres de dominio que se apoyan en una gran base de datos distribuida jerárquicamente por toda la red.

Este sistema divide la carga de gestión de un administrador central, repartiéndolo entre distintos subadministradores y éstos a su vez en otros subadministradores si fuera necesario. Este sistema de nombres de dominio se desarrolló debido a la gran expansión de máquinas conectadas al servicio. Debido a que es mucho más fácil el recordar un nombre que un número de 8 cifras, las empresas se pelean por tener posesión de esos nombres de dominio y poder llagar a más potenciales clientes o ya clientes a través de este sistema de telecomunicaciones cada día más en auge.

A raíz de la gran evolución del gran desarrollo de las telecomunicaciones y el gran número de ordenadores y conexiones existentes en la red en la actualidad se ha hecho necesario que un elemento que antes pasaba desapercibido como son los nombres de dominio haya pasado a ser un elemento a tener en cuenta para poder identificar y dar imagen a las marcas actuales. El gran paso se dio cuando los nombres de dominio pasaron de denominar ordenadores o terminales a denominar a marcas comerciales de las entidades que los poseían, dando a conocer el gran valor que estos nombres de dominio tienen en la sociedad actual.

Debido este gran auge y una vocación universal de Internet ha habido que poner unas reglas de juego para poder crear y estar en posesión de los nombres de dominio tratando de dar relevancia a razones como tener derechos legítimos para ser propietario del nombre, el derecho que se reconoce a las marcas famosas y notoriamente conocidas.

### a. Normativa dominios genéricos/regionales

Podemos clasificar a los nombres de dominio en dos tipos: los de primer nivel (son los que se encuentran en la escala de Internet en el nivel más alto) y los nombres de dominio de segundo nivel (aquellos que se pueden registrar bajo un nombre de dominio de primer nivel y que coinciden con el concepto que el solicitante desea ser reconocido en la Web).

Los nombres de dominio de primer nivel conocidos por las siglas TLD (Top Level Domain) son los que se sitúan al final de la dirección de Internet después del punto y que a su vez se dividen en dos tipos; de primer nivel genérico y los de primer nivel de código de país.

Los de primer nivel genéricos erán siete aunque en la actualidad ya son 14 y son:

- .com
- .net
- .org
- .mil
- .int
- .edu
- .gov
- .biz
- .info
- .pro
- .name
- .coop
- .aero

- .museum

Por otra parte tenemos los nombres de dominio de primer nivel de código de país que suelen estar compuestos de dos siglas relacionadas con las siglas de las normas ISO-3166.
Tenemos también el caso de las siglas de código de país relacionada con la Comunidad Económica Europea (.eu) que hacen mención a la CEE.

### 9.1 Inscripción de dominio

Para la asignación de nombres de dominio como puede ocurrir en el caso de que queramos solicitar un dominio para un centro escolar de primer nivel de código de país –es al tratarse de Centros ubicados en Castilla y León deberemos dirigirnos al Órgano competente en España ante tal inscripción:

1. Solicitud de la persona física o del representante legal en los demás supuestos, la solicitud puede presentarse en la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología (Disposición Adicional sexta de la Ley 11/1998 (1), General de las Telecomunicaciones) o electrónicamente (www.nic.es/solicitud). La solicitud podrá presentarse directamente por el solicitante o a través de un "agente registrador"; quien podrá asesorarlo (Art. 5.1 de la Orden, de 21 de marzo de 2000, conforme a la redacción formulada por el número tres de la Orden, de 12 de julio de 2001).

**LEY 11/1998, de 24 de abril, General de Telecomunicaciones**. ***Disposición adicional sexta***. La entidad pública empresarial de la Red Técnica Española de Televisión. 1. La Red Técnica Española de Televisión se configura como entidad pública empresarial, conforme a lo previsto en el artículo 43.1.b) de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Dicha entidad queda adscrita al Ministerio de Fomento, a través de la Secretaría General de Comunicaciones. 2. La entidad pública empresarial de la Red Técnica Española de Televisión tiene personalidad jurídica propia, plena capacidad de obrar y patrimonio propio y se regirá por lo establecido en esta disposición adicional, en su propio Estatuto, en la citada Ley 6/1997 y en las demás normas que le sean de aplicación. 3. Constituye el objeto de la entidad pública empresarial, la gestión, administración y disposición de los bienes y derechos que integran su patrimonio, correspondiéndole la tenencia, administración, adquisición y enajenación de los títulos representativos del capital de las sociedades en las que participe o pueda participar en el futuro. La entidad pública empresarial actuará, en cumplimiento de su objeto, conforme a criterios empresariales. Para el cumplimiento de su objeto, la entidad pública empresarial podrá realizar toda clase de actas de administración y disposición previstas en la legislación civil y mercantil. Asimismo, podrá realizar cuantas actividades comerciales o industriales estén relacionadas con dicho objeto, conforme a lo acordado por sus órganos de gobierno. Podrá actuar, incluso, mediante sociedades por ella participadas. 4. El régimen de contratación, de adquisición y de enajenación de la entidad se acomodará a las normas establecidas en derecho privado, sin perjuicio de lo determinado en la Ley 13/1995, de 18 de mayo, de Contratos de las Administraciones Públicas. 5. El régimen patrimonial de la entidad pública empresarial se ajustará a las previsiones del artículo 56 de la Ley 6/1997. No obstante, los actos de disposición y enajenación de los bienes que integran su patrimonio se regirán por el derecho privado. 6. La contratación del personal por la entidad pública empresarial se sujetará al derecho laboral, de acuerdo con las previsiones contenidas en el artículo 55 de la Ley 6/1997. 7. El régimen presupuestario, el económico-financiero, el de contabilidad, el de intervención y el de control financiero de la entidad pública empresarial será el establecido en la Ley General Presupuestaria, de acuerdo con lo previsto en el artículo 58 y en la disposición transitoria tercera de la Ley 6/1997. 8. La entidad pública empresarial se financiará con cargo a los Presupuestos Generales del Estado y mediante los ingresos derivados del ejercicio de su actividad. 9. Por acuerdo del Consejo de Ministros, se podrá convertir la entidad pública empresarial en sociedad mercantil.

2. El "agente" podrá encargarse de su tramitación. A estos efectos resulta de utilidad acudir a prestadores de servicios de nombres de dominio acreditados (www.007Names.com ; www.1stDomain.net ;), cuya relación puede consultarse en las páginas de cualquiera de los organismos y registros delegados de nombres de dominio (www.icann.org; www.setsi.mcyt.es ; www.internic.net; www.nic.es )
3. Se esperará a la aceptación o rechazo del nombre de dominio solicitado. Los nombres de dominio que cumplan las exigencias y no incurran en las prohibiciones ya señaladas serán asignados. Los nombres de dominio regulares se asignarán al primero que lo solicite. El nombre de dominio se inscribirá a favor de su titular en el Registro de los nombres y direcciones de dominio de Internet bajo el código de país correspondiente a España (.es), cuya gestión compete igualmente a "Red.es" (Disposición Adicional sexta, núm. 4.a) de la Ley 11/1998, General de las Telecomunicaciones).
4. A similares reglas procedimentales se somete la modificación, baja o cambio de dominio.

### 9.2 Recuperación de dominio

Puede ocurrir que a la hora de querer inscribir el Centro Escolar con un nombre de dominio similar o igual al mismo, este nombre de dominio esté ya utilizado, razón por la que daremos unas pautas de actuación ante tal inconveniente para poder intentar recuperar ese nombre de dominio al que tenemos derecho al tener derechos legítimos sobre el mismo. Los procedimientos que podemos llevar a cabo son:

**Medidas adoptadas para la solución de controversias**

Se plantearon varias soluciones ante esta situación, tales como la creación de un Tratado Internacional o la promulgación de Leyes nacionales, sin embargo ambas ideas fueron descartadas al no resultar viables. Entonces, la Organización Mundial de Propiedad Intelectual (OMPI) elaboró un informe contentivo de Recomendaciones relacionadas con los problemas que se plantean en el ámbito de los nombres de dominio, mismas que sirvieron de base para que la ICANN aprobara en 1999 la política uniforme de solución de controversias en materia de nombres de dominio. En España se aprobó la Orden de 12 de julio de 2001 por la que se modifica la Orden de 21 de marzo de 2000 por la que se

regula el sistema de asignación de nombres de dominio de Internet bajo el código de país correspondiente a España (es).

**Requisitos de la demanda:**

El sistema de resolución extrajudicial de conflictos sobre la utilización de nombres de dominio ".es", está desarrollado por la Entidad Pública Empresarial red.es. Está basado en las prácticas generalmente aplicadas en el ámbito internacional, y las recomendaciones surgidas por las entidades y organismos internacionales que desarrollan actividades relacionadas con la gestión del sistema de nombres de dominio de Internet.

Es necesario poseer derechos previos de un nombre de dominio ".es" ya asignado, para hacer uso de dicho sistema, de acuerdo a lo establecido en el Reglamento del Procedimiento de Resolución extrajudicial de conflictos, aprobado el 7 de noviembre de 2005 en su disposición adicional única.

Se deben acreditar todos los motivos por los que el registro del nombre de dominio ".es" es de carácter especulativo o abusivo, y en particular:

- Los motivos por los que el nombre de dominio ".es" es idéntico o similar hasta el punto de crear confusión con otro término sobre el que el Demandante alega poseer Derechos Previos; y
- Los motivos por los que debe considerarse que el Demandado carece de derechos o intereses legítimos sobre el nombre o nombres de dominio objeto de la demanda; y
- Los motivos por los que debe considerarse que el nombre de dominio ha sido registrado o se esté utilizando de mala fe.

En todo caso, la demanda debe ser instada ante un Proveedor de resolución extrajudicial de conflictos acreditado por la entidad pública empresarial red.es, de acuerdo al artículo 13 del Reglamento del Procedimiento de Resolución extrajudicial de conflictos.

En el sistema de resolución extrajudicial de conflictos de nombres de dominio ".es", hay varias figuras como son:

- Entidad pública empresarial red.es, en este caso sus funciones son básicamente, velar por el cumplimiento de las obligaciones de los Proveedores, y ejecutar las resoluciones establecidas por el experto.
- Proveedor, organización sin ánimo de lucro que administra las demandas, y vela por la tramitación de las mismas de acuerdo a lo establecido en el Reglamento, nombrado al Experto con imparcialidad e independencia.
- Experto: profesional con experiencia acreditada en resolución extrajudicial de conflictos, que resolverá la controversia con el máximo rigor e independencia, teniendo en cuenta el contenido de la demanda y la contestación a la misma.
- Partes: demandante, persona física u organización que insta la demanda ante el proveedor contra el demandado, titular del nombre de dominio ".es" objeto de la controversia.

No podrá ser iniciado el procedimiento de resolución extrajudicial de conflictos cuando se encuentre abierto un procedimiento de cancelación del nombre de dominio ".es". En todo caso la vía judicial está siempre abierta para las Partes, independientemente del estado de la demanda.

La tarifa establecida por los proveedores de resolución extrajudicial de conflictos de nombres de dominio ".es" es de 1.400€. En el caso de dominios genéricos es de 1500 dólares. Para que de comienzo el proceso lo primero de todo es abonar las tasas.

**Desarrollo de la Demanda**

Podrá iniciar un procedimiento de resolución extrajudicial de conflictos toda persona física o entidad jurídica presentando tres copias impresas y/o en formato electrónico de la Demanda ante el proveedor y una copia ante el organismo Red.es.

En la Demanda se deberá incluir al menos la siguiente documentación:

- El/los dominio/s objeto de la demanda

- El nombre, la dirección postal y de correo electrónico y los números de teléfono y de telefacsímil del Demandante o de representante autorizado por el Demandante en el procedimiento.

- El nombre del Demandado y toda la información conocida del Demandado para contactar con él pudiéndose dar también información que se tenía antes de la demanda.

- En su caso el Agente Registrador del Demandado antes de la Demanda.

- Descripción detallada de los Derechos previos en el que el Demandante fundamenta la Demanda aportando toda la información, copias de títulos o certificados que acrediten de forma fehaciente los Derechos previos.

- Una argumentación no superior a 5000 palabras con los motivos que acrediten el Registro de Dominio de Carácter especulativo o abusivo.

- Motivos por los que el nombre de dominio es idéntico o similar hasta el punto de crear confusión con otro término con el que el Demandante alegue poseer Derechos previos.

- Los motivos por los que debe considerarse que el Demandado carece de derechos previos o intereses legítimos de dominio objeto de la demanda.

- Los motivos por lo que debe considerarse que el nombre de dominio ha sido registrado o se esté utilizando de mala fe.

- La pretensión que se quiere obtener, es decir, la cancelación o el traspaso del dominio al Demandante.

- La identificación de cualquier procedimiento judicial, de verificación o cancelación, o de otra índole del que tenga conocimiento que se haya producido en relación al dominio demandado.

Al adherirnos a este sistema extrajudicial de conflictos se renuncia a los fueros que pudieran corresponder al Demandante y la sumisión expresa a la jurisdicción de los tribunales y juzgados. También se renuncia a cualquier acción judicial o de otra índole frente a Red.es, al Agente registrador, al Proveedor o al experto, así como a directores, funcionarios, empleados y agentes excepto de infracción dolosa o culposa.

Para resolver la demanda el experto tendrá en cuenta las declaraciones y documentos presentados por las partes.

El experto, en un plazo medio de 2 meses desde la interposición de la demanda, resolverá mediante resolución motivada que debe ser congruente con la pretensión de la demanda y no podrá decidir sobre cuestiones ajenas a la misma.

En base al artículo 13 apartado b subapartado 8 (1) de la instrucción por la que se regula el Derecho Recuperación del dominio bajo dominio "es" el demandante deberá indicar en la demanda la pretensión que se pretende obtener, es decir la transmisión del nombre de dominio al demandante o la cancelación del mismo.

Por tanto el experto puede resolver:

**Estimar la demanda**

En este caso el experto puede acordar:

1. Transmitir el nombre de dominio al demandante. En este supuesto, transcurrido el plazo máximo de un mes a partir de la notificación de la decisión a las partes y red.es, el demandante deberá enviar una solicitud de transmisión a transmisionDRP@nic.es. Recibida dicha solicitud se realizara la transmisión del nombre de dominio al demandante.

Solicitud de transmisión en cumplimiento de la resolución dictada en el procedimiento de resolución extrajudicial de conflictos:

- Para dominio gestionado por usuario final
- Autorización a Agente Registrador para actuar por cuenta del asignatario

2. Cancelar el nombre de dominio, que quedará para libre asignación. En el caso de que el demandante no haya indicado en la demanda que quiere la transmisión del nombre de dominio objeto de la controversia.

**(1) Reglamento de Procedimiento de resolución extrajudicial de conflictos para dominios "es" Orden ITC 1542/2005 de 19 de mayo de 2005**. ***Artículo 13*** apartado b subapartado 8 La pretensión que se pretende obtener, es decir la transmisión del nombre de dominio al Demandante o la cancelación del mismo;

**No estimar la demanda.**

En este supuesto el experto considera que el demandado tiene razón y por tanto el nombre de dominio debe continuar asignado a favor del antiguo titular.

Si en el citado plazo de 30 días, cualquiera de las partes notificará a Red.es un documento acreditando que se ha iniciado un procedimiento judicial ante un juzgado competente, red.es suspenderá la ejecución de la decisión hasta que reciba comunicación de que ha concluido dicho procedimiento judicial, salvo que el órgano judicial determine lo contrario.

## 10. Propiedad intelectual e industrial

### 10.1 Propiedad intelectual

Todos los bienes que se encuentran en la sociedad son objeto de protección de distintas maneras. En el caso de los objetos o bienes inmateriales como las ideas, las expresiones, las obras, un libro de crítica, un programa de ordenador,  es difícil establecer como protegerlos.

En países como Estados unidos esto se soluciona mediante las patentes que son muy difíciles de obtener en todos los sentidos, en tiempo y en dinero. En Europa se recurre a los Derechos Propios de la Propiedad intelectual. Estos Derechos se encuentran recogidos en nuestra legislación  centrada en el hecho de la intangibilidad del objeto que se desarrolla. Al tratarse de objetos que no se pueden coger ni guardar en una caja, se deben aplicar leyes con unas características específicas y desarrolladas adaptadas a las nuevas tecnologías tan arraigadas entre nosotros en la actualidad.

En la Unión Europea la protección y gestión de los derechos de autor y derechos afines es una cuestión que viene siendo de estudio desde al año 1995 pudiendo distinguir tres aspectos muy importantes a distinguir: 1º Los derechos materiales de autor, 2º La armonización en el ámbito de la defensa de los derechos y 3º La gestión de los Derechos. Una aproximación a estos tres aspectos se ha producido a través de la Directiva 2001/29/CE de l Parlamento Europeo y del Consejo de 22 de mayo relativa a la armonización de determinados aspectos de los derechos de autor en la sociedad de la información, cuyo función es lograr un mercado

interior de los derechos de autor y en los que se contemple la necesidad de atender a la digitalización de los derechos y los ajustes necesarios en la explotación de éstos.

Será objeto de la propiedad intelectual una obra literaria, artística o científica y la persona que gozará de está protección será el autor/es que generalmente será una persona natural o una persona jurídica si así lo reconoce la ley.

Las obras a su vez pueden ser independientes, en colaboración, colectivas o compuestas. Las obras independientes son aquellas que la creación es autónoma, aunque dicha obra sea publicada conjuntamente con otras; una obra en colaboración es aquella que sea un resultado unitario de varios autores, los derechos de autoría corresponden a todos y cada uno de los autores, además para poder modificarla es necesario el consentimiento de todos ellos; una obra es colectiva cuando la iniciativa y la coordinación de la misma es de una persona natural o jurídica que la edita y divulga bajo su nombre y está constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en un a creación única y autónoma sin que sea posible atribuir a alguno de ellos la autoría de una parte específica ya que forma la obra un conjunto; una obra es compuesta la obra nueva que incorpore una obra preexistente sin la colaboración del autor de ésta última, sin perjuicio de los derechos que a este corresponden y de su necesaria autorización.

Podemos distinguir dos tipos de derechos en relación a la propiedad intelectual y son por una parte los derechos personales o morales y por otra parte lo derechos patrimoniales. Los derechos morales o personales son irrenunciables e inalienables. Por otra parte los derechos patrimoniales pueden ser transmisibles.

Los derechos que el autor tiene desde que crea la obra duran hasta 70 años tras la muerte del artista tanto sean de textos como de software. En los centros escolares deberemos de tener cuidado con este aspecto en relación al software que utilicemos ya que podremos estar violando leyes al utilizar copias no autorizadas de programas. Este problema es más probable encontrarlo en los Centros Privados-Concertados ya que en los Centros Públicos es instalado y pagado los derechos por parte de la Consejería de Educación por parte de el Servicio de Informática perteneciente y pagado por la Junta de Castilla y León. Debemos de indicar a los Centros la necesidad de que exista una conservación de documentación en el Centro que

corrobore que son programas o software original que ya han sido pagados los derechos correspondientes para la utilización de los mismos.

La protección del software y más concretamente el software bajo el ámbito de los derechos de autor posee una serie de ventajas destacando:

- Plazo de protección: el plazo de los derechos de autor de 70 años tras su muerte frente a los 20 de las patentes.
- Copias no autorizadas: la protección que confieren los derechos de autor en principio cumplen mejor que las patentes este aspecto.
- Nacimiento de la protección en forma automática: esta protección nace de manera automática en cuanto la obra es creada o el software en este caso. En el caso de las patentes es necesaria una inscripción registral que no concede los derechos de manera automática ya que debe de examinarse la obra debiendo cumplir una serie de especificaciones técnicas.
- Pocas obligaciones para el titular: el titular de los derechos de autor no necesita cumplir con ningún requisito adicional a los propios de la creación cosa que no ocurre con las patentes ya que deben cumplir unos requisitos técnicos determinados.

Otro caso bien distinto es si nos referimos Al software libre que hace referencia a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el mismo. Además este tipo de software supone la libertad de distribuir copias de un programa por un distribuidor, con o sin modificaciones, gratis o a cambio de un precio.

Con los libros que utilizan los escolares no tendremos ningún tipo de problema ya que se están pagando derechos de autor para poder enseñar o aprender a los alumnos. En relación a los libros que suelen tener los Centros Escolares en las Bibliotecas escolares ya han sido pagados los derechos de autor ya que se suelen usar obras originales. En el caso de realizar reproducciones o copias de material escolar se deberá revisar que derechos tenemos y que autorizaciones deberemos requerir para cumplir con la Ley de Propiedad Intelectual.

En el caso de publicaciones realizadas por profesores con datos escolares deberemos comprobar que autorizaciones ha pedido al Centro para poder recabar los datos con los que

trabaja y si la propia Administración permite el uso de los datos para poder hacer publicaciones y que derechos y obligaciones tiene el autor de las mismas.

Además, cualquier obra susceptible de ser protegida mediante los derechos de autor puede además ser inscrita en el Registro General de la Propiedad Intelectual siendo potestativa, es decir, que al contrario que los derechos de Propiedad Industrial, no es necesaria la inscripción en el Registro para que la protección de la obra surta efecto.

### 10.2 Propiedad industrial

Los derechos de la Propiedad Industrial permiten la protección de determinados signos distintivos de la actividad empresarial, con el objeto de que las personas que acudan a unos servicios conozcan, que empresario o empresa se encuentran tras ellos.

En el caso de los Centros escolares lo único que podemos proteger es el símbolo o anagrama que suelen utilizar los Centros Escolares Privados-Concertados que representa a la Institución. Para tal efecto la Propiedad industrial defiende estos anagramas o símbolos que tanto valor tienen en un la imagen de un Colegio. En el caso de que queramos tener reconocidos los derechos de la Propiedad Industrial en relación a modelos y dibujos industriales y artísticos deberemos registrar tal modelo en la Oficina Española de patentes y marcas en el Departamento de Signos distintivos indicando que solicitamos una concesión de signos distintivos previo llamamiento a oposiciones y exámenes de oficio y en un plazo 12 meses sin suspenso ni oposiciones deben resolver y notificar el registro mencionado, en caso de que no notifiquen indica que se estima y se registra el signo.

Mediante la Ley 17/2001, de 7 de diciembre, se establece el régimen jurídico de los signos distintivos, marcas, rótulos de establecimiento y nombre comercial adecuando la legislación a los cambios producidos en relación a las Comunidades Autónomas, incorporar el ordenamiento comunitario e internacional, cambiar algunos procedimientos y adaptar el registro de marcas a la Sociedad de la Información.

### 10.3 Derecho “sui generis”

Mediante este derecho se reconocen los derechos propios sobre las bases de datos debido a la inversión sustancial evaluada cualitativa o cuantitativamente, realizada por el fabricante de cualesquiera medios tales como tiempo, esfuerzo, energía u otros similares para la obtención, verificación o presentación de su contenido. Este derecho también recae sobre las modificaciones sustanciales posteriores que se produjeran en una base de datos, siempre que las mismas cumplan todos los requisitos para el otorgamiento de dichos derechos a la misma. Este derecho surge en el momento en que finaliza el proceso de creación o fabricación de la base de datos y no con carácter previo al mismo teniendo una duración de 15 años desde el 1 de enero del año siguiente en que terminó dicho proceso de construcción.

En el caso de que en el Centro escolar se usen bases de datos debemos de cerciorarnos de que no violamos tal derecho y en el caso de que seamos nosotros los que hayamos creado dicha base de datos. Si que es verdad que podremos usar las bases de datos como se recoge en el Artículo 135 (1) de la Ley 5/1998, de 6 de marzo, de incorporación al Derecho Español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos de  excepciones al derecho "sui generis". En el apartado 1b que indica que cuando se trate de una extracción con fines ilustrativos de enseñanza o de investigación científica en la medida justificada por el objetivo no comercial que se persiga y siempre que se indique la fuente, aspecto a tener en cuenta por los docentes cuando se haga uso de las mismas.

## 11. Contratación informática

La contratación sobre bienes y servicio informáticos ha adquirido una relevancia incuestionable en la actividad empresarial, no sólo por su frecuencia sino también por su magnitud.

No caben dudas de que existen notas propias de la contratación de bienes y servicios informáticos y otras que, sin ser específicas, importan la puntualización de aspectos

**(1) LEY 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.** ***Artículo 135***. Excepciones al derecho “sui generis”. 1. El usuario legítimo de una base de datos, sea cual fuere la forma en que ésta haya sido puesta a disposición del público, podrá, sin autorización del fabricante de la base, extraer y/o reutilizar una parte sustancial del contenido de la misma, en los siguientes casos: a) Cuando se trate de una extracción para fines privados del contenido de una base de datos no electrónica. b) Cuando se trate de una extracción con fines ilustrativos de enseñanza o de investigación científica en la medida justificada por el objetivo no comercial que se persiga y siempre que se indique la fuente. c) Cuando se trate de una extracción y/o reutilización para fines de seguridad pública o a efectos de un procedimiento administrativo o judicial. 2. Las disposiciones del apartado anterior no podrán interpretarse de manera tal que permita su aplicación de forma que cause un perjuicio injustificado a los intereses legítimos del titular del derecho o que vaya en detrimento de la explotación normal del objeto protegido.

vinculados a institutos propios de la contratación corriente, tales como documentación técnica, concepto de conformidad, deberes de información y consejo, etc..

Estas notas, sin embargo, no implican reconocerle a los contratos informáticos una autonomía conceptual y sistemática respecto de contratos de otros géneros o que tengan diverso objeto.
La acepción contratos informáticos es amplia y podría generar la idea de que incluye no sólo los contratos en los cuales los bienes y servicios informáticos constituyen su objeto sino aquellos que se concluyen mediante bienes informáticos, como en el caso de la transferencia electrónica o la gama de operaciones telemáticas.
En tal sentido, resulta pertinente distinguir conceptualmente la contratación electrónica de la contratación informática.

Se denomina contratación electrónica o por medios informáticos aquella que se realiza mediante la utilización de algún elemento electrónico, con influencia decisiva, real y directa sobre la formación de la voluntad, el desenvolvimiento o la interpretación de un acuerdo.
En un sentido amplio esta clase de contratación comprende a todos los contratos que se celebran por medios electrónicos o telemáticos. En cambio, desde un punto de vista más restringido se consideran tales solamente a aquellos contratos que se celebran mediante la transmisión electrónica de datos de ordenador a ordenador.
En cambio, se entiende por contrato informático al que tiene por objeto bienes y servicios informáticos.
Los bienes informáticos comprenden tanto los “elementos materiales” que constituyen el soporte físico o hardware, su unidad central de procesamiento, periféricos, complementos, en definitiva todos los otros equipos que componen el soporte físico del elemento informático; como los 'bienes inmateriales' que proporcionan las órdenes, los datos, los procedimientos y las instrucciones en el tratamiento automático de información, cuyo conjunto constituye el soporte lógico del elemento informático.

En cambio, los servicios informáticos abarcan todos aquellos servicios que se relacionan con el tratamiento automatizado de la información y sirven de apoyo a la informática, tales como el diseño, el análisis y el mantenimiento del sistema.

El contrato existe desde que una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio. El contrato informático está comprendido dentro de la amplia definición del titulo ii de los contratos capitulo 1 en las Disposiciones generales en el artículo 1254 del Código Civil español, por el cual se considera que:
"*El contrato existe desde que una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio*".

El objeto de los contratos informáticos generalmente puede ser múltiple. Así, podemos mencionar como tal a:
a) bienes informáticos físicos/tangibles de:
1.- el Hardware o conjunto de dispositivos y elementos mecánicos, magnéticos, eléctricos y electrónicos del sistema;
2.- el Software o conjunto de bienes inmateriales que constituyen el soporte lógico del sistema, incluyendo los programas de base y las aplicaciones. Éste es entendido como el conjunto de afirmaciones o instrucciones para ser usadas directa o indirectamente en una computadora a fin de obtener un resultado determinado. (Public Law 96-517 (1980) de EE.UU.)
b) servicios informáticos de apoyo, como el diseño, el análisis y el mantenimiento de dicho sistema.
La diversidad de prestaciones en estos contratos es destacada por Pierre e Ives Poullet (1982), quienes señalan entre las prestaciones a que se puede obligar el proveedor, a las de: estudio y análisis de los problemas de automatización; suministro de equipo y software; adaptación de un software a las necesidades individuales del usuario, etc.

Al problema de la diversidad de prestaciones se añade la cantidad de posibles implicados. Además de los proveedores y usuarios pueden aparecer en la negociación del contrato: distribuidores, productores de equipos originales, entidades prestadoras de servicios y consultores en informática - del lado del productor -; y analistas de sistemas - por parte del usuario -

Los contratos informáticos pueden subsumirse en diversos tipos legales, como: de compraventa, outsourcing, de locación de obra o de servicios, de leasing y de licencia.

Sin embargo, se forman contratos al margen de los principios establecidos en la norma de nuestro código, comprendidos en la denominación especial de contratos 'innominados' o “atípicos”.

Un problema central de la teoría de los contratos atípicos es el régimen al que son sometidos. Según sea el criterio adoptado, se da prevalencia a las normas de los contratos típicos afines o bien, a las reglas generales de las obligaciones y de los contratos.

En múltiples aspectos el contrato informático se asemeja a los contratos clásicos; sin embargo, la complejidad de su estructura lo distingue de aquellos ya que en nuestro Derecho no tienen una regulación, debe ser buscada en la autonomía de las partes contratantes y de las normas especiales que puedan serle de aplicación.

### 11.1 Tipos de contratos más usuales

- **Contrato de Diseño de Sistemas de Información Proyecto y Consultoría:** Este tipo de contratos tiene por objeto la toma de datos, análisis, valoración y selección de sistemas de información (software y plataforma) con el fin de ajustarlo a las necesidades del cliente.
- **Contrato de Dirección y Ejecución de Proyectos:** Tiene por objeto la dirección y supervisión de la ejecución de trabajos establecidos en una Oferta o Consultoría previas.
- **Contrato de Montaje y Certificación de Redes:** Tiene por objeto la ejecución de trabajos de tendido de cableado y conexión de los elementos físicos necesarios para lograr el correcto medio de transmisión de los datos que deberá soportar el sistema. Puede tratarse de diversos tipos de redes (local, extensa, privada virtual, etc.)
- **Contrato de adquisición de Equipos informáticos:** Tiene por objeto la entrega de elementos físicos (hardware) que soportan los datos de una determinada instalación, señalándose como contraprestación la entrega de un precio. No diferenciamos en este caso los modos de adquisición (compraventa, renting, leasing, etc.).
- **Contrato de Adquisición de Sistemas Operativos. (Software de base)**: tiene por objeto la adquisición de la licencia para la utilización de los programas necesarios

para que funcione el software de aplicación. Tratándose de un producto normalmente conformado de antemano, se suele contemplar como contrato de adhesión.

- **Sistema de implementación se sistemas operativos (Software de base)**: tiene por objeto los servicios de instalación, parametrización, configuración, implantación y puesta en marcha del sistema operativo (monopuesto o redes). Puede tener múltiples niveles: perfiles de usuario, seguridad, planes de emergencia, auditorias, servicios de acceso remoto, etc.
- **Contrato de Adquisición (Software Horizontal):** tiene por objeto la adquisición de aplicaciones, que sin precisar alteración alguna, conjuntadas con el equipo físico, dan solución a necesidades de la generalidad de los usuarios (procesador de texto, hoja de cálculo, agenda, tratamiento de imágenes, etc.). Tratándose de un producto cerrado, se suele configurar como un contrato de adhesión.
- **Contrato de Adquisición (Software Vertical):** tiene por objeto la adquisición de aplicaciones que, conjuntadas con el equipo físico, dan solución a las necesidades específicas de un sector o grupo determinado (Gestión integrada de Empresas Industriales, Económico-Financiero, etc...). La aplicación base objeto del contrato suele ser adaptable a las necesidades del cliente dando lugar con ello al tipo de contrato más habitual dentro de los contemplados, y cargado de las implicaciones de la llamada teoría del contrato de resultado.
- **Contrato de Servicios (Análisis, Diseño y Programación a Medida)**: tiene por objeto la prestación de servicios de programación, propiamente dicha, de una aplicación diseñada específicamente para un cliente. Generalmente se componen de tareas de análisis, diseño y programación, pudiendo diferenciarse tres objetos distintos. Los problemas surgen sobre la titularidad, compartida o no, de los derechos de propiedad intelectual.

En el caso que nos ocupa, en los Centros escolares los contratos que más nos interesan y sobre todo en los Centros Privados Concertados ya que en los Públicos se ocupa La Consejería de Educación son los de Contrato de Servicios (Análisis, Diseño y Programación a Medida), Contrato de Adquisición (Software Horizontal), Contrato de Adquisición (Software Vertical), Contrato de adquisición de Equipos informáticos, Contrato de Adquisición de Sistemas Operativos. (Software de base) y de Sistema de implementación se sistemas

operativos (Software de base). Es por ello que indicaremos algunos aspectos a llevar a cabo a la hora de hacer la contratación:

**Contrato de Servicios (Análisis, Diseño y Programación a Medida)**

**Cláusulas específicas:** tener en cuenta todas las contempladas en el apartado de cláusulas en especial Derechos sobre el software, Propiedad, Cambios y modificaciones. Habrá que tener en cuenta la Legislación sobre Propiedad Intelectual, especial atención al modo de cesión de derechos y que la titularidad de los mismos esté suficientemente probada.

**Mantenimiento:** existen distintos tipos de mantenimiento que deberemos de tener en cuenta como son en las Redes y Sistemas Operativos en los Equipos Informáticos en el Software y en los Sistemas Gestores de Base de Datos.

Además deberán figurar en Anexos al Contrato los elementos a mantener especificando si se incluye Asistencia Técnica, Soporte a usuarios y Actualizaciones prestando especial atención a la documentación que deberá acompañarse con el envío de actualizaciones y diferenciando entre Garantía y Mantenimiento la fecha de entrada en vigor, la renovación tácita, la cláusula de revisión de precios, las cláusulas de resolución y rescisión, las penalizaciones por incumplimiento y la cesión y subarriendo del contrato.

### 11.1.1 Contrato de Adquisición (Software Horizontal)

**Cláusulas específicas:** deberemos hacer presentes en el contrato cláusulas que recojan el precio, el mantenimiento (actualizaciones), los derechos sobre el software, la compatibilidad, el manual y la documentación, entrenamiento y formación, soporte, garantías, la transmisión de derechos y la propiedad del mismo.

Además deberemos prestar atención en cuanto a la **i**mplantación**,** a la formación de usuarios**,** al mantenimiento (revisión), a las licencias OEM (Original Equipment Manufactured**)** y precargadas y si la apertura del paquete puede suponer la aceptación tácita de las condiciones contractuales.

### 11.1.2 Contrato de Adquisición (Software Vertical)

**Cláusulas específicas:** a tener en cuenta todas las contempladas en el apartado de cláusulas. Destacar la importancia del mantenimiento futuro. Revisar y prestar atención a los Anexos y Oferta, al control y seguimiento, la parametrización y por último al Feed-Back de la formación.

### 11.1.3 Contrato de adquisición de Equipos informáticos

**Cláusulas específicas**: especial atención a las cláusulas referentes al precio, al pago, a los repuestos, a las garantías, a la compatibilidad, a los manuales y Documentación y a la propiedad.

Los equipos deberán ser los adecuados para la aplicación, no por tratarse de equipos de "ultima generación" serán, ni los necesarios, ni los que mejor cumplan su cometido. Revisar los acuerdos OEM (Original Equipment Manufactured). Se trata de elementos incorporados de los que habitualmente no se entrega soporte para recarga en la documentación.

### 11.1.4 Contrato de Adquisición de Sistemas Operativos. (Software de base)

**Cláusulas específicas:** debemos de contemplar los derechos, el manual y documentación, el entrenamiento y formación, la compatibilidad, el soporte, la transmisión de derechos y la propiedad.
Además no tenemos que obviar las **v**ersiones OEM y precargadas.
Y recordar que el sistema operativo es la base el funcionamiento del sistema, por ello debe ser capaz de soportar y compatibilizarse con prácticamente la totalidad de aplicaciones existentes en el mercado; la apertura del paquete puede suponer la aceptación tácita de las condiciones contractuales por lo que antes de abrir se podría pedir una prueba del sistema.

### 11.1.5 Sistema de implementación de sistemas operativos (Software de base)

**Cláusulas específicas:** entre las cláusulas deben aparecer referencias al manual y documentación, el **e**ntrenamiento y formación, las pruebas de aceptación, la confidencialidad,

el soporte, los seguros, una definición de términos y conceptos y los cambios y modificaciones que pudieran producirse.
Por último, debemos exigir documentación específica del estado de la instalación.

Un aspecto que debemos de vigilar son las cláusulas que se incluyen en los contratos, revisando que no sean abusivas y que limiten nuestra capacidad de actuación en caso de un problema con el producto o servicio contratado.
Añadir que generalmente en el mundo de la informática suele realizarse contratos de adhesión en los que una de las partes fija las cláusulas del contrato y la otra parte se adhiere a las mismas; suelen ser contratos de contratación en masa y se suelen violar los derechos de los consumidores de bienes y servicios informáticos ya que no existe una emisión libre de voluntad, una de las partes es la que pone las condiciones y la otra parte o ase adhiere o no recibe los servicios sin posibilidad de negociar las cláusulas.

Además sería correcto tener en cuenta las siguientes recomendaciones para adecuar las cláusulas antes citadas y evitar los futuros problemas:

- Obligaciones claras, concretas y concisas.
- Referencia a la oferta, siempre que sea posible, la cual convendrá esté recogida como uno de los Anexos al contrato.
- Deber de asesoramiento (normalmente se habrá realizado en la fase precontractual).
- En el caso de ejecución por parte de diversos proveedores bajo la figura de cesión o subarriendo, deberá prestarse especial importancia a la asunción de responsabilidades por cada uno de ellos.
- Aclaración de términos y conceptos: Si se emplean abreviaturas deben ser traducidas en perfecto castellano, caso de no tener posible traducción, deberán acompañarse de la necesaria explicación o definición sobre el alcance de su inclusión en contrato debido a que suelen venir en inglés o idiomas como el chino o japonés.

## 11.2 Fases de los contratos informáticos

La contratación informática, por su propia naturaleza requiere de un proceso de formación del consentimiento que tiende a dilatarse en el tiempo, dando lugar a dos fases claramente diferenciadas:

- Precontractual o de formación del objeto en la que será necesario un asesoramiento técnico siendo muy recomendable definir previamente las necesidades que deben cubrirse contando con la opinión de profesionales en materia informática. Existen Consultores Homologados por Organismos Oficiales o Compañías de reconocido prestigio (Como por ejemplo Davara&Davara consultores) que ofrecen una metodología de trabajo con el fin de definir la solución informática que dé respuesta a las necesidades planteadas. No podemos olvidar que la contratación informática debe apoyarse de manera fundamental en la buena fe de las partes y, por ello, el proveedor tiene el deber de aconsejar, en su caso, al cliente, analizando previamente sus necesidades, con el fin de definir cuál será el conjunto de bienes, aplicaciones y servicios que se precisen, informándole de las diversas posibilidades existentes, siendo lo más importante, las tendencias futuras presumibles del mercado a las que deberá tener la necesidad de adaptarse.
- Contractual en la que se deberá contar con un correcto asesoramiento jurídico estrictamente necesario en todo negocio jurídico complejo. La situación que suele darse en el mercado es que el proveedor, con ánimo comercial, exagera la calidad del bien o servicio, y a su vez el cliente, sin formación y asesoramiento necesarios, se forma una imagen de panacea a sus problemas, que no se ajusta a la realidad, y que sólo se despejará a la hora de tener que aclarar sus diferencias ante peritos o tribunales que establecerán, si es posible, qué es lo que se contrató. A ello hemos de añadir que debido a la generación de conceptos novedosos (ADSL, RDSI, ciberespacio,...) se están generando nuevas clases de relaciones jurídicas que desconocemos si en el futuro seguirán siendo reconducidas a figuras jurídicas ya existentes.

## 12. Firma electrónica

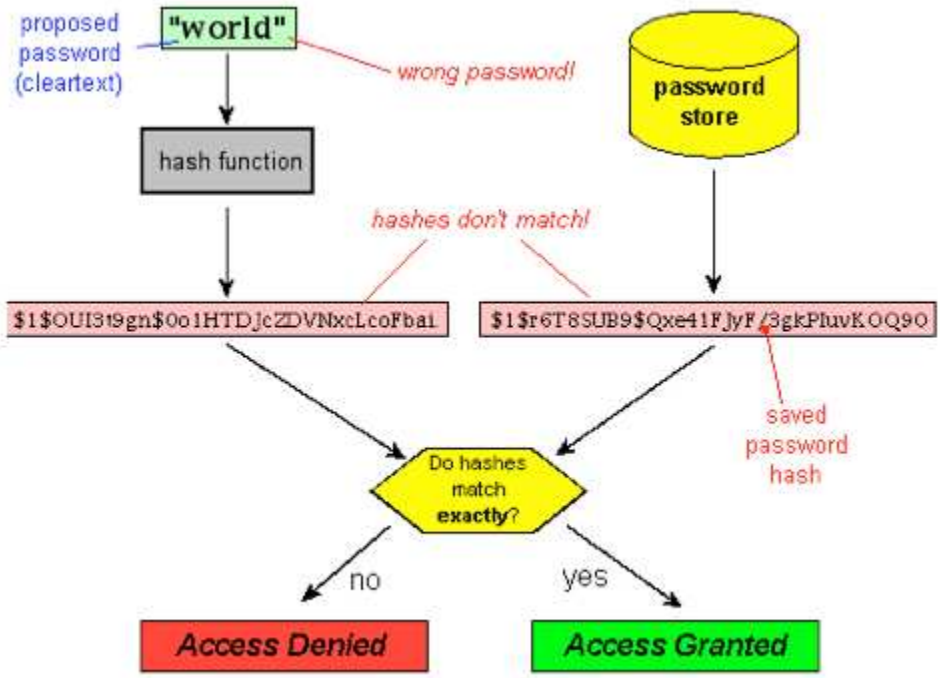
El 19 de diciembre de 2003 fue publicado en el BOE la Ley 59/2003, de 19 de diciembre, de firma electrónica. Esta ley se compone de 36 artículos agrupados en seis títulos, diez disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales con una amplia exposición de motivos en la que se explica y clarifica la entrada de esta nueva ley que tanto tardó tras la presentación de varios borradores. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación".

Por tanto la Firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos que pueden ser utilizados como medio de identificación del firmante. Por otra parte la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma con validez jurídica reconocida.

En la firma electrónica avanzada se introduce la necesidad de tener dos claves, una clave Pública (vinculada al firmante de manera única y a los datos a los que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control) y una clave Privada (que el firmante nunca hace pública). Por último añadir un nuevo concepto que es el de la Firma electrónica avanzada y reconocida que añade a la firma electrónica avanzada la necesidad de estar basada en un certificado reconocido y haber sido generada mediante un dispositivo seguro de creación de firma.

Las funciones y características principales de la firma electrónica son:

- No repudio, es decir, ninguna de las partes firmantes puede negar haber realizado el envío, aspecto que mejora a la firma manuscrita que puede ser repudiada.
- Integridad del contenido, es decir, el mensaje no puede ser modificado en el camino ya que la función “hash” es la que garantiza que existan modificaciones en el mismo.
- Autenticación del contenido, el contenido del mensaje se asocia a los autores como ellos lo dispusieron en un principio.
- Confidencialidad, es decir, el contenido debe ser secreto entre las partes.
- Identificación de las partes, los firmantes son aquellos que dicen ser, aspecto que garantiza la firma electrónica avanzada reconocida.




Funcionamiento del Sistema “Hash”

Fuente: library.thinkquest.org/.../images/hashing3.jpg

Como se establece en el artículo 3 del apartado 4 de la Ley de firma electrónica 59/2003: “*la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel*”.

En los Centros Escolares podemos hacer uso de la firma electrónica reconocida para llegar a acuerdos y tratos de manera electrónica ahorrando en tiempo y dinero al poder realizar los trámites de manera sencilla y rápida. Además debemos incidir en la importancia de la ley 59/2003 en la que se reconoce un nuevo papel que es el reconocimiento de la firma electrónica de las personas jurídicas. En la práctica, este reconocimiento indica que se otorga a un tercero la capacidad de representar a la persona jurídica, y además éste pueda delegar y usar esta firma por otra persona por lo que se suscita el problema del buen uso de la firma de la persona jurídica y de las responsabilidades que subyacen y quien es el responsable en caso de incumplimiento y como se depurarían las responsabilidades. Este aspecto también puede y debe ser tenido en cuenta y atribuir a alguien la responsabilidad de su uso pero limitando que acciones pueden ser realizadas por el que tenga la firma de manera única y que acciones

requerirán de más integrantes que supervisen lo que se está firmando con la citada firma. Además deberá indicarse que consecuencias tendrá el uso indebido de la firma electrónico del Centro indicando sanciones como embargos, perdidas de trabajo o remuneraciones en su caso.

Para poder utilizar el la firma electrónica reconocida deberemos realizar tres pasos:

1. Solicitud del certificado
2. Acreditación de la identidad mediante personación física en una oficina de registro.
3. Descarga del certificado desde Internet.


1. Solicitud del certificado

Fuente: Fábrica Nacional de Moneda y Timbre


3. Descarga del certificado desde Internet.

Fuente: Fábrica Nacional de Moneda y Timbre

## 13. Aspectos tributarios/Fiscalidad electrónica y administración

El empleo de las tecnologías de la información en las actividades comerciales ha dado lugar a importantes cambios, algunos de ellos de naturaleza jurídica. Y entre ellos adquieren gran importancia los relacionados con la fiscalidad, ya que el comercio electrónico genera un gran número de transacciones financieras susceptibles de tributación.

Los tributos gravan manifestaciones de capacidad económica y es evidente que en el comercio electrónico se producen hechos que pueden ser considerados como tales.

Si bien es cierto que el comercio electrónico no puede ser concebido como una fórmula fácil para defraudar, no lo es menos que en la práctica se plantean numerosos problemas que es preciso resolver.

Para llegar a conclusiones válidas sobre estas cuestiones es conveniente referirse, en primer lugar, a los tributos que gravan el comercio electrónico. Nos centraremos en los más importantes: por un lado los impuestos que recaen sobre la renta (Impuesto sobre la Renta de las Personas Físicas, Impuesto sobre la Renta de los No Residentes, y el Impuesto sobre Sociedades) y por otro el Impuesto sobre el Valor Añadido que grava el consumo. En la contratación electrónica inciden también otros tributos, aunque en menor medida.

En segundo lugar, se analizarán los problemas que plantea la aplicación efectiva de estos tributos, así como sus posibles soluciones. Destacan, entre otros, la dificultad para localizar las actividades comerciales y la calificación jurídica de las operaciones realizadas y de las rentas obtenidas.

La fiscalidad del pago por medios electrónicos, por la importancia que éstos están adquiriendo en la sociedad actual, merece especial atención.

### 13.1 Tributos que gravan el comercio electrónico

Los tributos que gravan el comercio electrónico son los mismos que se aplican en la actualidad al comercio tradicional: Impuesto sobre la Renta de las Personas Físicas (IRPF),

Impuesto sobre la Renta de los No Residentes, Impuesto sobre Sociedades e Impuesto sobre el Valor Añadido (IVA). Estos impuestos, los tres que recaen sobre la renta y el que grava el consumo, son los que afectan de forma más directa al comercio, pero también inciden en la contratación otros tributos como los Impuestos Especiales, el Impuesto sobre Transmisiones Patrimoniales y los Impuestos Aduaneros.

Es importante tener en cuenta que en caso de que España tenga suscrito con el país de residencia del preceptor de las rentas un Convenio para evitar la doble imposición, dicho convenio tiene primacía sobre el derecho interno, por lo que se aplicará de acuerdo con su contenido, que está normalmente inspirado en el modelo Convenio de Doble Imposición de la OCDE. En caso de que no exista Convenio con el país de residencia del preceptor de las rentas, se aplicará la Ley del impuesto sobre la renta de no residentes, cuyos criterios de interpretación deberán estar en concordancia con las normas reguladoras del IRPF y del impuesto sobre sociedades.

**El impuesto sobre la renta de las personas Físicas (IRPF)**

El Impuesto sobre la Renta de las Personas Físicas es la obtención de renta por el contribuyente, que debe ser una persona física con residencia habitual en España. Los criterios para considerar que una persona tiene su residencia habitual en España son los siguientes:

- Permanencia en su territorio más de 183 días al año
- Ubicación en ella del núcleo principal de sus intereses económicos
- En caso de traslado a un paraíso fiscal, se considerará que el contribuyente sigue residiendo en España en el año del cambio y en los cuatro siguientes.

La base imponible del impuesto está compuesta por los rendimientos del trabajo, del capital mobiliario, del capital inmobiliario, y los de las actividades económicas, además de por las ganancias y pérdidas patrimoniales y las imputaciones de renta. Lógicamente son los rendimientos de actividades económicas los que están relacionados directamente con la fiscalidad del comercio electrónico.

Es evidente que cuando quien lleva a cabo sus actividades económicas a través de la red es una persona física con residencia en España, los rendimientos obtenidos serán objeto de gravamen en este impuesto.

**El impuesto sobre la renta de no residentes**

El Impuesto sobre la Renta de No Residentes grava las rentas obtenidas en territorio español por las personas físicas y entidades no residentes en el mismo. Para que las rentas obtenidas tributen en España es preciso que concurra alguna de las siguientes circunstancias:

- Las actividades o explotaciones económicas sean realizadas en territorio español.
- Que se trate de prestaciones de servicios utilizadas en territorio español, en particular las referidas a la realización de estudios, proyectos, asistencia técnica o apoyo a la gestión.
- También, y como no, deben incluirse entre las rentas sometidas a tributación las derivadas del comercio electrónico, siempre que se cumplan los requisitos a los que nos hemos referido.

**El impuesto sobre sociedades**

El Impuesto sobre Sociedades grava las rentas obtenidas por las sociedades y demás entidades jurídicas. El hecho imponible está constituido precisamente por la obtención de esas rentas, siendo indiferente su fuente u origen. Por lo que, al igual que ocurría con los anteriores impuestos, no hay ninguna razón para excluir las obtenidas en el comercio electrónico.

En este impuesto se consideran entidades residentes en España las que cumplan cualquiera de los siguientes requisitos:

- Su constitución se hubiera realizado conforme a las leyes españolas.
- Su domicilio social se halle en territorio español.
- Que tengan la sede dirección efectiva en dicho territorio. Se entiende por ésta el lugar en el que radica la dirección y control del conjunto de sus actividades.

**Impuestos aduaneros**

Por Impuestos Aduaneros debemos entender todos aquellos que tienen como objeto el tráfico internacional de mercancías. En la actualidad son tributos de regulación comunitaria. La figura más importante que se incluye en ellos es la de los derechos a la importación, tributo que se exige por la entrada de mercancías en el territorio aduanero comunitario. Pero además se incluyen en ellos las siguientes figuras: regímenes aduaneros suspensivos; exacciones reguladoras agrícolas y demás gravámenes a la importación exigibles en el marco de la política agrícola común; derechos antidumping y antisubvención y los derechos menores.

Una vez más, si los bienes objeto de estos impuestos no circulan por la red, es irrelevante el carácter electrónico del contrato. Pero cuando se trata de suministros on line surgen dificultades, sobre todo porque esos bienes no atravesarán la aduana físicamente. La solución que se viene propugnando pasa por la exención de los Impuestos Aduaneros de los bienes digitalizados.

**Impuesto sobre el Valor Añadido**

El Impuesto sobre el Valor Añadido es un impuesto indirecto (los tres anteriores son directos) que recae sobre el consumo y grava las entregas y prestaciones de servicios efectuadas por empresarios o profesionales (operaciones interiores), las adquisiciones intracomunitarias de bienes y las importaciones de bienes. Las entregas de bienes y prestaciones de servicios deben ser realizadas por empresarios o profesionales a título oneroso, con carácter habitual u ocasional, en el desarrollo de su actividad empresarial o profesional.

La contratación electrónica es susceptible de incluirse en cualquiera de los tres supuestos, con lo que el comercio electrónico no puede considerarse excluido de la aplicación de este impuesto.

El artículo 84.2 de la ley 37/1992, de 28 de diciembre sobre el Impuesto del Valor Añadido establece que "a los efectos de lo dispuesto en esta Ley, "*se considerarán establecidos en territorio de aplicación del Impuesto, los sujetos pasivos que tengan en el mismo la sede de su actividad económica, un establecimiento permanente o su domicilio fiscal, aunque no*

*realicen las operaciones sujetas al impuesto desde dicho establecimiento*". Por otro lado, el artículo 69.2 de la misma Ley sitúa la sede de la actividad económica "*en el territorio donde el interesado centralice la gestión y el ejercicio habitual de su actividad empresarial o profesional, siempre que carezca de establecimientos permanentes en otros territorios*".

Surgen aquí los mismos problemas que en la imposición directa: dudas sobre si se puede considerar como establecimiento permanente un servidor o una página Web, dificultades al aplicar el criterio de la sede de dirección de la actividad económica; y sobre todo, problemas técnicos para las Administraciones tributarias en la localización de los sujetos intervinientes en una contratación electrónica. Esto último se debe principalmente a la falta de correspondencia entre los nombres de dominio y una situación geográfica concreta, y a las posibilidades de anonimato con que cuentan los adquirentes en Internet.

En principio, la localización de las operaciones comerciales electrónicas en el IVA dependerá de la calificación de las mismas como adquisición de bienes (operaciones internas), adquisición intracomunitaria, régimen de ventas a distancia, importación o prestación de servicios.

En el primer caso, según el artículo 68.1 Ley sobre el Impuesto del Valor Añadido, las operaciones se entenderán realizadas en territorio de aplicación del impuesto cuando los bienes se pongan a disposición del adquirente en dicho territorio. Si se trata de una adquisición intracomunitaria de bienes, el adquirente (que debe ser empresario o profesional) será el sujeto pasivo del impuesto y habrá de practicar la auto repercusión del mismo.

Si el producto objeto de la compraventa electrónica procede de países no pertenecientes a la Unión Europea, su introducción en España será considerada importación sujeta al IVA, liquidando en Aduana la cuota impositiva correspondiente (artículo 18 Ley sobre el Impuesto del Valor Añadido).

En la contratación electrónica de prestaciones de servicios hay que tener en cuenta el artículo 69 Ley sobre el Impuesto del Valor Añadido, que establece la regla general para la localización de las prestaciones de servicios en el territorio donde el prestador de los mismos tenga la sede de su actividad económica o, en su defecto, en el domicilio de quien los preste.

## 13.2 Fiscalidad del pago por medios electrónicos

Los medios de pago electrónicos pueden causar importantes problemas a las Administraciones tributarias porque facilitan la utilización de bancos establecidos en paraísos fiscales. Hace unos años, evadir dinero a estos lugares resultaba, además de complicado, caro. En la actualidad, se puede acceder a ellos con una simple transacción electrónica.

En relación con los aspectos tributarios del sistema bancario virtual que utiliza paraísos fiscales para captar depósitos a través de Internet, se aplica la normativa destinada a las operaciones realizadas con o por personas residentes en paraísos fiscales. Tiene especial importancia el artículo 17.2 de la Ley de Impuesto sobre Sociedades:

"*La Administración tributaria podrá valorar por su valor normal de mercado las operaciones efectuadas con o por entidades residentes en países o territorios calificados reglamentariamente como paraísos fiscales cuando la valoración convenida hubiera determinado una tributación en España inferior a la que hubiere correspondido por aplicación del valor normal de mercado o un diferimiento de dicha tributación*".

## 14. Documento de Seguridad aplicado a los Centros Escolares Públicos y Privado-Concertados

En los centros en los que se aplicará este tipo de documento de seguridad se aplicarán medidas de seguridad de nivel Básico, nivel medio y nivel alto, podemos también usar medidas de tipo básico para los datos personales que sólo requieran este tipo de medidas y utilizar las medidas de los tres tipos en cuanto estemos tratando datos personales especialmente protegidos (1).

**Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999 de 11 de junio de 1999** CAPÍTULO II Medidas de seguridad de nivel básico Artículo 8. Documento de seguridad. 1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. 2. 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, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento. c) Funciones y obligaciones del personal. 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. 3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. 4. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. Artículo 9. Funciones y obligaciones del personal. 1. Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el artículo 8.2.c). 2. El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento. Artículo 10. Registro de incidencias. El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma. Artículo 11. Identificación y autenticación. 1. El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso. 2. 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. 3. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible. Artículo 12. Control de acceso. 1. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. 2. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados. 3. La relación de usuarios a la que se refiere el artículo 11.1 de este Reglamento contendrá el acceso autorizado para cada uno de ellos. 4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero. Artículo 13. Gestión de soportes. 1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad. 2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero. Artículo 14. Copias de respaldo y recuperación. 1. El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. 2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. 3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. CAPÍTULO III Medidas de seguridad de nivel medio Artículo 15. Documento de seguridad. El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado. Artículo 16. Responsable de seguridad. El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento. Artículo 17. Auditoría. 1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años. 2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas. 3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos. Artículo 18. Identificación y autenticación. 1. El responsable del fichero establecerá 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. 2. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Artículo 19. Control de acceso físico. Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal. Artículo 20. Gestión de soportes. 1. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, 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 informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada. 3. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario. 4. Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos. Artículo 21. Registro de incidencias. 1. En el registro regulado en el artículo 10 deberán consignarse, además, 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. 2. Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos. Artículo 22. Pruebas con datos reales. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado. **CAPÍTULO IV.- MEDIDAS DE SEGURIDAD DE NIVEL ALTO** Reglamento de Medidas de Seguridad de ficheros automatizados Artículo 23.- Distribución de soportes. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte. Artículo 24.- Registro de accesos. 1.- De cada acceso se guardarán, 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. 2.- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. 3.- Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación de los mismos. 4.- El período mínimo de conservación de los datos registrados será de dos años. 5.- El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y

elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes. Artículo 25.- Copias de respaldo y recuperación. Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento. Artículo 26.- Telecomunicaciones. La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

## MODELO DOCUMENTO DE SEGURIDAD

## DOCUMENTO DE SEGURIDAD DE (Colegio o Centro Educativo)

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 994/1999 de 11 de Junio), recogen las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal.

Los ficheros de datos: **TRABAJADORES**, **ALUMNOS, PROVEEDORES** en adelante el fichero, descrito en el documento de Notificación a la Agencia de Protección de Datos, se encuentra oficialmente clasificado como de nivel de seguridad medio en el caso de los trabajadores y de nivel alto para los alumnos al tratarse datos especialmente protegidos, atendiendo a las condiciones descritas en el articulo 4 apartado 3 y 4 del Real Decreto citado, siendo por tanto aplicable a él todas las medidas de seguridad de nivel medio y nivel alto que se establecen en el Capitulo II del citado decreto.

El contenido principal de este documento queda estructurado como sigue:

### CAPÍTULOS.

- **CAP.I:** Ámbito de aplicación del documento.
- **CAP.II:** Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
- **CAP.III:** Procedimiento general de información al personal.
- **CAP.IV:** Funciones y obligaciones del personal.

- **CAP.V:** Procedimientos de notificación y respuesta ante las incidencias.
- **CAP.VI:** Procedimientos de revisión.
- **CAP.VII:** Consecuencias del incumplimiento del documento de seguridad.

**ANEXOS.**

- **ANEXO I. a.** Aspectos relativos al fichero trabajadores.
- **ANEXO I. b.** Aspectos relativos al fichero estructura.
- **ANEXO I. c.** Aspectos relativos al fichero.
- **ANEXO II.** Nombramientos.
- **ANEXO III.** Autorizaciones salida o recuperación de datos.
- **ANEXO IV**. Inventario de soportes.
- **ANEXO V.** Registro de incidencias.
- **ANEXO VI.** Encargados de tratamiento.
- **ANEXO VII.** Registros de entrada y salida de soportes.
- **ANEXO VIII.** Funciones y responsabilidades.
- **ANEXO IX.** Modificaciones introducidas en este documento.
- **ANEXO X.** Plantilla recibí.

**Este documento deberá mantenerse permanentemente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.**
**En el apartado referente a las claves de acceso debemos informarles de que las claves se actualizan cada 7 días para cada usuario, en el caso de este informe se han incluido las primeras claves facilitadas por el responsable de seguridad.**

CAPITULO I: ÁMBITO DE APLICACIÓN DEL DOCUMENTO.

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de (Nombre del titular o del centro educativo) incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de

carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

En concreto los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente son los siguientes:

- Fichero de Nominas y RRHH (nivel medio).
- Fichero de Profesores y Trabajadores (nivel medio)
- Fichero de alumnos (datos especialmente protegidos)

En el Anexo I se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

**CAPITULO II: MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTANDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO**.

- Medidas y normas relativas a la identificación y autentificación del personal autorizado a acceder a los datos personales.

En los ficheros de nominas y rrhh y clientes-proveedores, la identificación de los usuarios se realizará de forma inequívoca y personalizada, verificando su autorización, así como se limitará la posibilidad de intentar reiteradamente el acceso al sistema informático.

-Control de acceso.

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones.
Exclusivamente ((Nombre del Centro escolar Titular de los ficheros) está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.
Exclusivamente el personal autorizado podrá conceder, anular o alterar el acceso sobre los datos y recursos.
Relación de usuarios actualizada con acceso autorizado a cada sistema de información. Así mismo se incluye el tipo de acceso autorizado para cada uno de ellos.

## FICHERO NOMINAS Y RECUROS HUMANOS

### RESPONSABLE DEL FICHERO

| Nombre y apellidos | Cargo | Alta | Baja |
|---|---|---|---|
| | APODERADO | | |

**RESPONSABLE DE SEGURIDAD**

| Nombre y apellidos | Cargo | Alta | Baja |
|---|---|---|---|

| | | | |
|---|---|---|---|
| | DIR. ADMINISTRACION | | |

**ADMINISTRADORES DEL SISTEMA**

| **Nombre y apellidos** | **Organismo / Unidad Administrativa** | **Alta** | **Baja** |
|---|---|---|---|
| | DPTO. INFORMÁTICO | | |

**USUARIOS DEL FICHERO**

| Nombre y apellidos | Unidad Administrativa | N1 inventario Puesto Trabajo | Alta | Baja |
|---|---|---|---|---|
| | ADMINISTRACION PERS. | | | |
| | ADMINISTRACION PERS. | | | |
| | ADMINISTRACION PERS. | | | |
| | ADMINISTRACION PERS. | | | |
| | | | | |
| | ADMINISTRACION PERS. | | | |
| | OUTSOURCING | | | |
| | SELECCIÓN | | | |
| | ADMINISTRACION PERS. | | | |
| | SELECCIÓN | | | |
| | SELECCIÓN | | | |
| | ADMINISTRACION PERS. | | | |
| | OUTSOURCING | | | |
| | OUTSOURCING | | | |
| | ADMINISTRACION PERS. | | | |
| | RECEPCION | | | |
| | ADMINISTRACION PERS | | | |

| | | | | |
|---|---|---|---|---|
| | RECEPCION | | | |
| | | | | |

**ADMINISTRADORES DEL SISTEMA**

| Nombre y apellidos | Organismo / Unidad Administrativa | Alta | Baja |
|---|---|---|---|
| | DPTO. INFORMÁTICA | | |

**USUARIOS DEL FICHERO**

| Nombre y apellidos | Unidad Administrativa | N1 inventario Puesto Trabajo | Alta | Baja |
|---|---|---|---|---|
| | DEPT. COMPRAS | | | |
| | DEPT. COMPRAS | | | |
| | DEPT. COMPRAS | | | |
| | DEPT. COMPRAS | | | |

## **CONTROL DE ACCESO FÍSICO**:

Exclusivamente el personal que se indica a continuación, podrá tener acceso a los locales donde se encuentran ubicados los sistemas de información correspondientes a los ficheros.

| PUESTOS DE TRABAJO | CONTROL DE ACCESO | OFICINA |
|---|---|---|
| **ADMINISTRACIÓN** | **PRESENCIAL** | |
| **SELECCIÓN** | **PRESENCIAL** | |
| **FINANCIERO** | **PRESENCIAL** | |
| **GERENCIA** | **PRESENCIAL** | |
| **LIMPIEZA** | **PRESENCIAL** | |

Los locales donde se ubiquen los ordenadores que contienen el Fichero deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos, especialmente en el caso de que el Fichero esté ubicado en un servidor accedido a través de una red.

- Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del Fichero que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

- El acceso a los locales donde se encuentre el fichero deberá estar restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico.

## CONTROL DE SOPORTES.

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el Fichero.

Dado que la mayor parte de los soportes que hoy en día se utilizan, como disquetes o CD-ROM, son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos del Fichero tiene el control de estos medios.

- Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

    - Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

- Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero.

- La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero, utilizando para ello el documento adjunto.

- El responsable del Fichero mantendrá un Libro de registro de entradas y salidas donde se guardarán los formularios de entradas y de salidas de soportes , con indicación de tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío, destinatario, o persona responsable de la recepción que deberán estar debidamente autorizadas.

- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas

necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

## **ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES**.

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Si se tratan ficheros con datos especialmente protegidos deberá realizarse cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

## RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al fiche tratado. El método de control de salida de ficheros se añade a continuación.

| **REGISTRO Y AUTORIZACIÓN DE SALIDA DE SOPORTES** | |
|---|---|
| Fecha y hora de salida del soporte | |

| **SOPORTE** | |
|---|---|
| Tipo de soporte y número | DVD UNA UNIDAD CADA 15 DÍAS |
| Contenido | FICHEROS RELATIVOS A NOMINAS – RRHH –ALUMNOS (DEL CENTRO ESCOLAR) |
| Ficheros de donde proceden los datos | BASE DE DATOS DE (CENTRO ESCOLAR) |
| Fecha de creación | |

| **FINALIDAD Y DESTINO** | |
|---|---|
| Finalidad | PROTECCIÓN DE DATOS REFERENTES A NOMINAS-RRHH Y ALUMNOS (CENTRO ESCOLAR) |
| Destino | (DIRECCIÓN DEL CENTRO ESCOLAR) |
| Destinatario | (Nombre y apellidos del responsable del fichero) |

| **FORMA DE ENVÍO** | |
|---|---|
| Medio de envío | (Tipo de soporte utilizado, papel, pen drive, CD, DVD, correo interno etc…) |
| Remitente | (Nombre del centro escolar) |
| Precauciones para el transporte | En función de los datos personales que se utilicen (especialmente protegidos o no cifrando la información) |

| **AUTORIZACIÓN** | |
|---|---|
| Persona responsable de la entrega | RESPONSABLE DE MENSAJERÍA INTERNA |
| Persona que autoriza | (Nombre del responsable de gestión de registro y autorización de soportes) |
| Cargo / Puesto | (Cargo/Centro escolar titular) |
| Observaciones | |
| Firma | |

**<u>En el Anexo X se incluye un formulario de autorización creado para facilitar el control y seguimiento de los documentos enviados.</u>**

**<u>Ficheros temporales.</u>**

Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

## Copias de seguridad.

Es obligatoria realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la perdida o destrucción.

Las recuperaciones de datos de los ficheros NOMINAS-RRHH Y ALUMNOS, deberán ser autorizadas por el Responsable del Fichero.

## Responsable de seguridad.

El responsable del fichero designará a o los responsables de seguridad, que con carácter general se encargarán de coordinar y controlar las medias definidas en este documento.

En ningún caso, la designación supone una delegación de la responsabilidad que corresponde al Responsable del Fichero.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de desempeño de su cargo Una vez transcurrido el periodo, el responsable del fichero podrá nombrar al mismo responsable de seguridad o a otro diferente.

## Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado.

## CAPITULO III: PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el capitulo siguiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas a través de una copia de este documento donde se exponen las normas que se deben cumplir y las consecuencias de no hacerlo. Para asegurar la entrega de este documento se añadirá un “recibí” que deberá ser consignado con fecha hora y firma del empleado/a que viene recogido en el anexo IX

## CAPITULO IV: FUNCIONES Y OBLIGACIONES DEL PERSONAL.

**Funciones y obligaciones de carácter general.**

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación personal notificas al responsable del fichero o de seguridad, las incidencias de las que tengan conocimiento respecto a los recursos protegidos.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y responsabilidades descritas en el ANEXO VIII.

## CAPITULO V: PROCEDIMIENTO DE NOTIFICACIÓN Y RESPUESTA ANTE LAS INCIDENCIAS.

Se considerarán como “incidencias de seguridad”, entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de (Nombre del Centro escolar titular de los ficheros)

El procedimiento a seguir para la notificación de incidencias será el de registrarla en el Libro de Incidencias o comunicarlas al Responsable de Seguridad.

El registro de incidencias se gestionará mediante notificación manual a través de un impreso adjunto en el anexo V.

## CAPITULO VI: PROCEDIMIENTOS DE REVISIÓN.

El documento de seguridad deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, deberán, adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los dato de carácter personal.

Los cambios y revisiones se especificarán en el Anexo IX.

## CAPITULO VII: CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD.

- La veracidad de los datos contenidos en los anexos de este documento, así como el cumplimiento de las normas que contiene, deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías.

- El responsable de seguridad del Fichero comprobará, con periodicidad, que la lista de usuarios autorizados se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Además de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

- Se comprobará también con periodicidad, la existencia de copias de respaldo que permitan la recuperación de Fichero que deberán realizarse al menos una vez a la semana o cuando se produzcan cambios en los ficheros con datos personales del tipo que sean.

- A su vez, y también con periodicidad, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

- El responsable de seguridad, verificará, con periodicidad, el cumplimiento de lo previsto en relación con las entradas y salidas de datos, sean por red o en soporte magnético. De cada acceso se guardarán, 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.

- El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad las incidencias registradas en el libro correspondiente, para independientemente de las

medidas particulares que se hayan adoptado en el momento que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.

- Al menos con carácter bienal, se realizará una auditoria, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoria serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

- Los resultados de todos estos controles periódicos, así como de las auditorias serán adjuntados a este documento de seguridad.

- El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

## ANEXO I a. ASPECTOS RELATIVOS AL FICHERO *NOMINAS Y RRHH*
## Actualizado a (Fecha de actualización).

- **Nombre del fichero**: Fichero Nominas y RRHH.
- **Unidades con acceso al fichero**: Dto. Administración, Dto. Selección y Dto. Outsourcing, Dirección.
- **identificador y nombre del fichero**: FICHERO Nominas y RRHH
  **Nombre:** FICHERO Nominas y RRHH.

**Descripción**: fichero destinado a la contratación de trabajadores y tratado de las nóminas que en el caso de Centros Concertados se envían a la Consejería de Educación.

- **Nivel de medidas de seguridad**: NIVEL MEDIO
- **Responsable de Seguridad**: Nombre del Centro Escolar
- **Administrador**: Nombre y apellidos
- **Leyes o regulaciones que afecten al fichero**:15/1999 //1720/2007
- **Estructura del fichero principal**: DNI-NIF, Nª seguridad social, nombre, apellidos, dirección, teléfono, firma en la solicitud de empleo, estado civil, familia, fecha de nacimiento, lugar de nacimiento, sexo, nacionalidad, situación militar, licencias o permisos, formación, experiencia profesional, profesión, puestos de trabajo, historial del trabajador, datos bancarios, subsidios o beneficios.
- **Información sobre el fichero o tratamiento**: la finalidad de este fichero es la contratación de personas, todas aquellas personas que soliciten trabajo, están obligadas a suministrar sus datos personales. Las cesiones previstas de estos datos serán las relativas a las que se realicen de cara a la contratación a las empresas cliente. No se realizan transferencias internacionales. La procedencia de los datos: a través de auto candidaturas, envío de C.V y el INEM. El procedimiento de recogida de datos es a través de formularios en papel (solicitud de empleo) e Internet. El soporte utilizado es: papel, informático, telemático.
- **Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición**: Nombre del Centro Escolar y Dirección física completa
- **Descripción del sistema de información**: programa de gestión de personal. Trabajamos con sistema operativo (Ejemplo Windows Xp, Vista, 7).
- **Descripción detallada de las copias de seguridad**: DVD o soporte que se utiliza distinto del ordenador donde se encuentran los ficheros
- **Funciones del personal con acceso a los datos personales**:

El personal afectado por esta normativa se clasifica en dos categorías

- Administradores del sistema, encargados de administrar o mantener el entorno operativo del fichero. Por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos saltándose las barreras de acceso de la Aplicación

- Usuarios del fichero, o personal que usualmente utiliza el sistema informático de acceso al fichero

- Responsable de seguridad del fichero, que servirá de enlace con el Responsable del Fichero sin que suponga una delegación de responsabilidades

Anexo VIII: funciones y responsabilidades.

- **Descripción de los procedimientos de control de acceso e identificación:**
- **Relación actualizada de usuarios con acceso autorizado:**

**RESPONSABLE DEL FICHERO**

| Nombre y Apellidos | Cargo | Clave | Alta | Baja |
|---|---|---|---|---|
| | APODERADO | | | |

**RESPONSABLE DE SEGURIDAD**

| Nombre y Apellidos | Cargo | Clave | Alta | Baja |
|---|---|---|---|---|
| | DIR. ADMINISTRACION | | | |

**ADMINISTRADORES DEL SISTEMA**

| Nombre y Apellidos | Organismo/Unidad Administrativa | Alta | Baja |
|---|---|---|---|
| | DPTO. INFORMÁTICA | | |

## USUARIOS DEL FICHERO

| Nombre y Apellidos | Unidad Administrativa | Puesto de Trabajo | Clave | Alta | Baja |
|---|---|---|---|---|---|
| | ADMINISTRACION | ADMON. | | | |
| | ADMINISTRACION | ADMON | | | |
| | ADMINISTRACION | DIR. ADMON. | | | |
| | ADMINISTRACION | ADMON. | | | |
| | ADMINISTRACION | ADMON. | | | |
| | OUTSOURCING | ADMON | | | |
| | SELECCIÓN | ADMON | | | |
| | ADMINISTRACION | ADMON | | | |
| | SELECCIÓN | SELECCIÓN | | | |
| | SELECCIÓN | SELECCIÓN | | | |
| | ADMINISTRACION | ADMON. | | | |
| | OUTSOURCING | ADMON | | | |
| | OUTSOURCING | ADMON | | | |
| | ADMINISTRACION | ADMON | | | |
| | ADMINISTRACION | ADMON. | | | |
| | RECEPCION | RECEPCIÓN | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## ANEXO I b: ASPECTOS RELATIVOS AL FICHERO ALUMNOS

**Actualizado a (Fecha).**

- **Nombre del fichero**: Fichero alumnos
- **Unidades con acceso al fichero**: Dpto. Alumnos
- **Identificador y nombre del fichero**: FICHERO alumnos
  **Nombre:** FICHERO alumnos
  **Descripción**: FICHERO DESTINADO A la gestión del alumnado.
- **Nivel de medidas de seguridad**: NIVEL ALTO
- **Responsable de Seguridad**: NOMBRE CENTRO ESCOLAR
- **Administrador**: NOMBRE DEL ADMINISTRADOR
- **Leyes o regulaciones que afecten al fichero**:15/1999
- **Estructura del fichero principal**: DNI-NIF, Nº seguridad social, nombre y apellidos, dirección y teléfono, estado civil, familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, formación, datos bancarios, beneficios, datos ideológicos, datos de salud, datos de informes médicos y psicológicos.
- **Información sobre el fichero o tratamiento**: la finalidad de este fichero es el uso interno del centro escolar con objeto de desarrollo de la actividad con el alumnado. Las personas obligadas a suministrar los datos son los alumnos que accedan a recibir formación educativa con carácter obligatorio y con Fondos Públicos Indicar las cesiones siempre con consentimiento expreso y las transferencias internacionales que se prevean en el caso de intercambio de alumnos. La procedencia de dichos datos es por parte del propio alumnado y el soporte utilizado es informático.
- **Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición**: Centro escolar con dirección completa
- **Descripción del sistema de información**: programa de gestión ya sean ofimáticos como los facilitados por la Consejería de Educación y para las notas de alumnos. Sistemas operativos utilizados. **Descripción detallada de las copias de seguridad**:DVD´S

- **Información sobre conexión con otros sistemas**: este fichero no está relacionado con el resto de los ficheros ya que hay datos especialmente protegidos.
- **Funciones del personal con acceso a los datos personales**:

El personal afectado por esta normativa se clasifica en dos categorías

- Administradores del sistema, encargados de administrar o mantener el entorno operativo del fichero. Por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos saltándose las barreras de acceso de la Aplicación

- Usuarios del fichero, o personal que usualmente utiliza el sistema informático de acceso al fichero
- Responsable de seguridad del fichero, que servirá de enlace con el Responsable del Fichero sin que suponga una delegación de responsabilidades

Anexo VIII: funciones y responsabilidades.

**Descripción de los procedimientos de control de acceso e identificación:**

- **Relación actualizada de usuarios con acceso autorizado:**

**RESPONSABLE DEL FICHERO**

| Nombre y Apellidos | Cargo | Clave | Alta | Baja |
|---|---|---|---|---|
| | APODERDO | | | |

**RESPONSABLE DE SEGURIDAD**

| Nombre y Apellidos | Cargo | Clave | Alta | Baja |
|---|---|---|---|---|
| | DIR. ALUMNADO | | | |

**ADMINISTRADORES DEL SISTEMA**

| Nombre y Apellidos | Organismo/Unidad Administrativa | Alta | Baja |
|---|---|---|---|
| | DPTO. INFORMÁTICA | | |

USUARIOS DEL FICHERO

| Nombre y Apellidos | Unidad Administrativa | Puesto de Trabajo | Alta | Baja |
|---|---|---|---|---|
| | DEPT. GESTIÓN ALUMNADO | ADMON | | |
| | DEPT. GESTIÓN ALUMNADO | ADMON | | |
| | DEPT. GESTIÓN ALUMNADO | ADMON | | |
| | DEPT. GESTIÓN ALUMNADO | ADMON | | |

## ANEXO II: NOMBRAMIENTOS.

Nombramientos que afecten a los perfiles incluidos en este documento, por ejemplo: responsable de seguridad.

Para hacer efectivos los nombramientos se debe firmar la siguiente plantilla de compromiso con los deberes y obligaciones que recoge la ley de Protección de Datos vigente.

- Adjuntamos un documento de aceptación del cargo y de las responsabilidades que implica el mismo.

**Yo don/doña……..con DNI……a fecha……..acepto el cargo de…… y me comprometo a cumplir los deberes y obligaciones así como todas responsabilidades que este nombramiento implica.**

**Firma:…**

## ANEXO III: AUTORIZACIONES SALIDA O RECUPERACIÓN DE DATOS.

Cualquier salida de soportes fuera de los locales donde está ubicado el fichero deberá ser autorizada por el responsable del fichero con el documento que se adjunta.

El Responsable del fichero mantendrá un Libro en el que se registrará las salidas de soportes, cuyos asientos estarán constituidos por los documentos de autorización de salida debidamente cumplimentados.

| **REGISTRO Y AUTORIZACIÓN DE SALIDA DE SOPORTES** |
|---|

| | |
|---|---|
| Fecha y hora de salida del soporte | |

| **SOPORTE** | |
|---|---|
| Tipo de soporte y número | |
| Contenido | |
| Ficheros de donde proceden los datos | |
| Fecha de creación | |

| **FINALIDAD Y DESTINO** | |
|---|---|
| Finalidad | |
| Destino | |
| | |

| | |
|---|---|
| Destinatario | |

| **FORMA DE ENVÍO** | |
|---|---|
| Medio de envío | |
| Remitente | |
| Precauciones para el transporte (datos encriptadas) | |

| **AUTORIZACIÓN** | |
|---|---|
| Persona responsable de la entrega | |
| Persona que autoriza | |
| Cargo / Puesto | |
| Observaciones | |
| Firma | |

El responsable del fichero mantendrá un Libro en el que se registrará las entradas de soportes cuyos asientos estarán constituidos por los datos recogidos en el formulario que se adjunta.

La persona responsable de la recepción de soportes estará debidamente autorizada por el responsable del fichero.

| **REGISTRO DE ENTRADA DE SOPORTES** | |
|---|---|
| Fecha y hora de entrada de soporte | |

| **SOPORTE** | |
|---|---|
| Tipo de soporte y número | |
| Contenido | |
| Fecha de creación | |

| **ORIGEN Y FINALIDAD** | |
|---|---|
| Finalidad | |
| Origen | |

| **FORMA DE ENVÍO** | |
|---|---|
| Medio de envío | |

| | |
|---|---|
| Remitente | |
| Precauciones para el transporte | |

| **AUTORIZACIÓN** | |
|---|---|
| Persona responsable de la recepción | |
| Cargo / Puesto | |
| Observaciones | |
| Firma | |

**ANEXO IV: INVENTARIOS DE SOPORTES.**

Este punto debe contener los siguientes procedimientos:

- Asignación y cambio de contraseñas.
- Procedimiento de respaldo y recuperación.
- Procedimiento de gestión de soportes: identificación de etiquetas, inventario de soportes, lugar de almacenamiento, y en el caso de eliminación de los mismos, se indicará el método utilizado.

| **Fichero: NOMBRE DE FICHERO** | | | | | |
|---|---|---|---|---|---|
| ALTAS | | BAJAS | | | |
| | | Reutilización | Destrucción | MÉTODO | |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |
| / | / / | | | | / / |

## ANEXO V: REGISTRO DE INCIDENCIAS.

Cuando ocurre una incidencia, el usuario o administrador deberá registrarla en el Libro de Incidencias o comunicarla al Responsable de Seguridad para que a su vez proceda a su registro.

Se describirá el procedimiento de notificación y gestión de incidencias:

En la notificación se hará constar: el tipo de incidencia, la fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que pueden producir la incidencia y descripción de tallada de la misma.

**Impreso de notificación de incidencias**

| | |
|---|---|
| Incidencia N1: **\|_____\|** ( Este número será rellenado por el Responsable de seguridad) | |
| Fecha de notificación: **/__/__/____/** | |
| Tipo de incidencia**:** | |
| Descripción detallada de la incidencia: | |
| Fecha y hora en que se produjo la incidencia: | |
| Persona(s) a quien(es) se comunica**:** | |
| Efectos que puede producir**:** (En caso de no subsanación o incluso independientemente de ella) | |

| |
|---|
| Recuperación de Datos :( A rellenar sólo si la incidencia es de este tipo)<br><br>Procedimiento realizado:<br><br><br>Datos restaurados:<br><br><br>Datos grabados manualmente:<br><br>Persona que ejecutó el proceso:<br><br>Firma del Responsable del fichero:<br><br>Fdo _____ |
| Persona que realiza la comunicación:<br>Fdo.:_____ |

**ANEXO VI: ENCARGADOS DE TRATAMIENTO.**

No es necesario en este caso puesto que no hay un acceso de un tercero a los datos del responsable del fichero.

**ANEXO VII: REGISTRO DE ENTRADA Y SALIDA DE SOPORTES.**

| **REGISTRO Y AUTORIZACIÓN DE SALIDA DE SOPORTES** | |
|---|---|
| Fecha y hora de salida del soporte | |

| **SOPORTE** | |
|---|---|
| Tipo de soporte y número | |
| Contenido | |
| Ficheros de donde proceden los datos | |
| Fecha de creación | |

| **FINALIDAD Y DESTINO** | |
|---|---|
| Finalidad | |
| Destino | |
| Destinatario | |

| **FORMA DE ENVÍO** | |
|---|---|
| Medio de envío | |
| Remitente | |
| Precauciones para el transporte | |

| |
|---|

| AUTORIZACIÓN | |
|---|---|
| Persona responsable de la entrega | |
| Persona que autoriza | |
| Cargo / Puesto | |
| Observaciones | |

| REGISTRO DE ENTRADA DE SOPORTES | |
|---|---|
| Fecha y hora de entrada de soporte | |

| SOPORTE | |
|---|---|
| Tipo de soporte y número | |
| Contenido | |
| Fecha de creación | |

| ORIGEN Y FINALIDAD | |
|---|---|
| | |

| | |
|---|---|
| Finalidad | |
| Origen | |

| **FORMA DE ENVÍO (Datos encriptadas en ficheros con Datos Especialmente Protegidos)** | |
|---|---|
| Medio de envío | |
| Remitente | |
| Precauciones para el transporte | |

| **AUTORIZACIÓN** | |
|---|---|
| Persona responsable de la recepción | |
| Cargo / Puesto | |
| Observaciones | |
| Firma | |

## ANEXO VIII: FUNCIONES Y RESPONSABILIDADES.

### FUNCIONES DEL RESPONSABLE DEL FICHERO

El responsable del fichero es el encargado jurídicamente de la seguridad del fichero y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

Designará al responsable de seguridad.

### FUNCIONES DEL RESPONSABLE DE SEGURIDAD

Es el encargado de coordinar y controlar las medidas definidas en el presente documento.

### CLASIFICACIÓN DEL PERSONAL DE ADMINISTRACIÓN O PERSONAL INFORMÁTICO

Se distinguen dos situaciones diferentes, que condicionan el tipo de personal que tiene acceso al fichero en cada caso:

-Producción habitual, sin incidencias técnicas. Explotación diaria.
-Errores, cortes, incidencias técnicas de cualquier tipo que detienen la producción.

### PERSONAL AUTORIZADO EN PRODUCCIÓN HABITUAL

En el primer caso, el acceso se limita a los siguientes perfiles

-Usuario / administrador del sistema.
-Operador.

### ADMINISTRADORES TÉCNICOS E INFORMÁTICOS GENERALES QUE INTERVIENEN EN SITUACIONES NO HABITUALES

Cuando no existe un personal técnico determinado que se pueda relacionar de forma directa con un fichero o sistema informático y que acceda habitualmente al mencionado fichero o sistema.

Siempre será posible conocer el personal que intervino con posterioridad a la intervención, dejando constancia de ello, identificando al personal técnico, anotándolo en le Registro de Incidencias.

## FUNCIONES DE LOS ADMINISTRADORES O PERSONAL INFORMÁTICO

El personal que administra el sistema de acceso al Fichero se puede a su vez clasificar en varias categorías, que no necesariamente deberán estar presentes en todos los casos, siendo en algunas ocasiones asumidas por una misma persona o personas. Estas categorías son:
- Administradores (Red, Sistemas operativos y Bases de Datos). Serán los responsables de los máximos privilegios y por tanto de máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al software (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.

- Operadores (Red, Sistemas operativos, Bases de Datos y Aplicación). Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener acceso directo a los datos del Fichero, ya que su actuación no precisa de dicho acceso.

- Mantenimiento de los sistemas y aplicaciones. Personal responsable de la resolución de incidencias que puedan surgir en el entono hardware / software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.

- Cualquier otro que la organización establezca.

## OBLIGACIONES DEL RESPONSABLE DEL FICHERO

Implantar las medidas de seguridad establecidas en este documento.

El responsable del Fichero deberá garantizar la difusión de este Documento entre todo el personal que vaya a utilizar.

Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según los artículos 8 y 9 de la Normativa de Seguridad.

Deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

Deberá designar uno o varios responsables de seguridad.

**Entorno de Sistema Operativo y de Comunicaciones**

El responsable del Fichero aprobará o designará al administrador que se responsabilizará del sistema operativo y de comunicaciones.

En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero.

**Sistema Informático o aplicaciones de acceso al Fichero**

El responsable del fichero se encargará de que los sistemas informáticos de acceso al Fichero tengan su acceso restringido mediante un código de usuario y una contraseña.

Asimismo cuidará que todos los usuarios autorizados para acceder al Fichero, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

**Salvaguarda y protección de las contraseñas personales**

Sólo las personas relacionadas, podrán tener acceso a los datos del Fichero.

**Gestión de soportes**

La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero.

**Entrada y salida de datos por red**

Todas las entradas y salidas de datos del Fichero que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el responsable del Fichero. Igualmente si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

**Procedimientos de respaldo y recuperación**

El responsable del Fichero se encargará de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.

Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

**Controles periódicos de verificación del cumplimiento**

El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

Al menos cada dos años, se realizará una auditoria, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoria serán analizados por el responsable

de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

Los resultados de todos estos controles periódicos, así como de las auditorias serán adjuntados a este documento de seguridad.

## OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

El responsable de seguridad coordinará la puesta en marcha de las medidas de seguridad, colaborará con el responsable del fichero en la difusión del Documento de seguridad y cooperará con el responsable del fichero controlando el cumplimiento de las mismas.

**Gestión de incidencias**

El responsable de seguridad habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

Analizara las incidencias registradas, tomando las medidas oportunas en colaboración con el responsable del Fichero.

**Controles periódicos de verificación del cumplimiento**

El responsable de seguridad del Fichero comprobará, con una periodicidad, que la lista de usuarios autorizados se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Además de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

Se comprobará también al menos con periodicidad, la existencia de copias de respaldo que permitan la recuperación de Fichero.

A su vez, y también con periodicidad, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

El responsable de seguridad, verificará, con periodicidad, el cumplimiento de lo previsto en los apartados de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

Al menos cada dos años, se realizará una auditoria, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoria serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

Los resultados de todos estos controles periódicos, así como de las auditorias serán adjuntados a este documento de seguridad.

## OBLIGACIONES QUE AFECTAN A TODO EL PERSONAL

### Puestos de trabajo

Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los

datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos.

En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.

Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo al autorización del responsable de seguridad o por administradores autorizados.

**Salvaguarda y protección de las contraseñas personales**

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.

**Gestión de incidencias**

Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al administrador del sistema, o en su caso del registro de la misma en el sistema de registro de incidencias del Fichero.

El conocimiento y la no notificación de una incidencia por parte de un usuario serán considerados como una falta contra la seguridad del Fichero por parte de ese usuario.

**Gestión de soportes**

Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos

periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero.

Cuando la salida de datos del Fichero se realice por medio de correo electrónico los envíos se realizaran, siempre y únicamente, desde una dirección de correo controlada por el administrador de seguridad, dejando constancia de estos envíos en el directorio histórico de esa dirección de correo o en algún otro sistema de registro de salidas que permita conocer en cualquier momento los envíos realizados, a quien iban dirigidos y la información enviada. Además serán cifrados los datos enviados.

Cuando los datos del Fichero deban ser enviados fuera del recinto físicamente protegido donde se encuentra ubicado el Fichero, bien sea mediante un soporte físico de grabación de datos o bien sea mediante correo electrónico, deberán ser encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.

Se deberán registrar mediante correo electrónico o transferencia de datos por red, de forma que se pueda siempre identificar su origen, tipo de datos, formato, fecha y hora del envío y destinatario de los mismos.

## OBLIGACIONES DE LOS ADMINISTRADORES Y PERSONAL INFORMÁTICO

### Entorno de sistema operativo y de Comunicaciones

Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado.

En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados.

El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.

Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

**Sistema Informático o aplicaciones de acceso al Fichero**

Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

En cualquier caso se controlarán los intentos de acceso fraudulento al Fichero, limitando el número máximo de intentos fallidos, y, cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha, hora, código y clave errónea que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al Fichero se utilizasen datos reales, se deberá aplicar a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero, y se deberán relacionar esos ficheros de prueba.

**Salvaguarda y protección de las contraseñas personales**

Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

**Procedimientos de respaldo y recuperación**

Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

Estas copias deberán realizarse una periodicidad, a salvo en el caso de que no se haya producido ninguna actualización de los datos.

En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo.

Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

**Controles periódicos de verificación del cumplimiento**

El responsable de seguridad del Fichero comprobará, con periodicidad, que la lista de usuarios autorizados se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de

acceso al administrador o administradores del Fichero. Además de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

Se comprobará también al menos con periodicidad, la existencia de copias de respaldo que permitan la recuperación de Fichero.

A su vez, y también con periodicidad, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de lo mismo

El responsable de seguridad, verificará, el cumplimiento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

Al menos cada dos años, se realizará una auditoria, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoria serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

Los resultados de todos estos controles periódicos, así como de las auditorias serán adjuntados a este documento de seguridad.

**ANEXO IX: MODIFICACIONES INTRODUCIDAS EN ESTE DOCUMENTO.**

| **Versión** | **Fecha** | **Actualizaciones** |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | | |
| | | |

## ANEXO X: PLANTILLA RECIBÍ

| NOMBRE | Fecha | FIRMA |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

**Bibliografía**


- Código Civil.
- Código de Comercio.
- Constitución española Aprobada por Las Cortes en sesiones plenarias del Congreso de los Diputados y del Senado celebradas el 31 de octubre de 1978.
- Davara Rodríguez, M. A., " *Factbook comercio electrónico*", Aranzadi, Cizur Menor, 2004.
- Davara Rodríguez, M. A., "*Análisis del Real Decreto 1720/2007"*: El reglamento de la LOPD, DAFEMA, , 2008.
- Decreto 17/2005, de 10 de febrero, modificado por el Decreto 8/2007, de 25 de enero, por el que se regula la admisión del alumnado en centros docentes sostenidos con fondos públicos de la Comunidad de Castilla y León; por la Orden EDU/184/2005, de 15 de febrero, modificada en varias ocasiones por la Orden EDU/133/2007, de 1 de febrero, la Orden EDU/2075/2008, de 27 de noviembre, y la Orden EDU/2380/ 2009, de 23 de diciembre.
- Decreto 8/2007 de 25 de enero febrero por el que se regula la admisión de alumnado a centros educativos financiados por fondos públicos de la Comunidad de Castilla y León.
- DECRETO 51/2007, de 17 de mayo, por el que se regulan los derechos y deberes de los alumnos y la participación y los compromisos de las familias en el proceso educativo, y se establecen las normas de convivencia y disciplina en los Centros Educativos de Castilla y León.
- Decreto 17/2005 de 10 de febrero por el que se regula la admisión de alumnado a centros educativos financiados por fondos públicos de la Comunidad de Castilla y León.
- Dictamen 1/2009 sobre las propuestas que modifican la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad Ley Orgánica 2/2006, de 3 de mayo, de Educación.
- Directiva 2000/31/CE del Parlamento Europeo y de Consejo del 8 de junio.

- 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 (Directiva sobre la privacidad y las comunicaciones electrónicas)
- Documento de trabajo 1/08 sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios).
- Ley Orgánica 5/2000, reguladora de la responsabilidad penal de los menores.
- Ley 40/1998, de 9 de diciembre del Impuesto sobre la Renta de las Personas Físicas y otras Normas Tributarias.
- Ley 7/98 de 13 de Abril, sobre Condiciones Generales de la Contratación.
- Ley 26/84 de 19 de Julio, General para la Defensa de los Consumidores y Usuarios.
- Ley 3/91 de 10 de Enero, de Competencia Desleal.
- Ley 26/91 de 21 de Noviembre, sobre Contratos Celebrados Fuera de Establecimientos Mercantiles.
- Ley 17/89 de 17 de Julio, de Defensa de la Competencia.
- Ley 22/94 de 6 de Julio, de Responsabilidad Civil por los daños causados por productos defectuosos.
- Ley 7/95 de 23 de Marzo, de Crédito al Consumo.
- Ley 17/2001, de 7 de diciembre, de marcas.
- LEY 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.
- Ley Orgánica 8/1985, de 3 de julio, Reguladora del Derecho a la Educación.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- ley 37/1992, de 28 de diciembre sobre el Impuesto del Valor Añadido.
- Ley 7/96 de 15 de Enero, de Ordenación del Comercio Minorista.
- Ley 11/1998, General de las Telecomunicaciones.
- Ley 1/96 de 12 de Abril, de Propiedad Intelectual.
- Ley 34/2002 de 11 de julio de Servicios de Sociedad de la Información de Comercio Electrónico.
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

- LEY 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio.
- Ley 5/98 de Protección de Bases de Datos, reflejo y transposición de la Directiva 96/9 CEE.
- ORDEN de 14 de febrero de 1996, por la que se regula el procedimiento para llevar a cabo la evaluación psicopedagógica y se establece el dictamen y los criterios de escolarización de los alumnos con necesidades educativas especiales.
- ORDEN EDU/1774/2009, de 28 de agosto, por la que se crea el fichero automatizado de datos de carácter personal de la Consejería de Educación denominado «Sistema integrado de becas y ayudas al estudio».
- ORDEN EDU/1951/2007, de 29 de noviembre, por la que se regula la evaluación en la educación primaria en Castilla y León.
- ORDEN EDU/1774/2009, de 28 de agosto, por la que se crea el fichero automatizado de datos de carácter personal de la Consejería de Educación denominado «Sistema integrado de becas y ayudas al estudio».
- Pierre e Ives Poullet, 'Les contrats informatiques: Reflexions sur dix ans de jurisprudence belge et francaise', " Droit et Practique du Commerce international ", 1982, Nº 1, p. 87.
- Plan sectorial de oficio a la enseñanza reglada no universitaria.
- Política uniforme de solución de controversias en materia de nombres de dominio Política aprobada el 26 de agosto de 1999 Documentos de ejecución aprobados el 24 de octubre de 1999.
- R.D.18281999, de 3 de Diciembre, por el que se aprueba el Reglamento del Registro de Condiciones Generales de la Contratación.
- Reglamento del Registro de la Propiedad Intelectual. 773/1993 de 14 de Mayo.
- Real Decreto 732/1995 de 5 de mayo por el que se establecen los derechos y deberes de los alumnos y las normas de convivencia en los centros.
- Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999.
- Real Decreto 732/1995 de 5 de mayo "Derechos y deberes de los alumnos y normas de convivencia en centros docentes no universitarios".

- Reglamento de Procedimiento de resolución extrajudicial de conflictos para dominios “es” Orden ITC 1542/2005 de 19 de mayo de 2005.
- REAL DECRETO LEGISLATIVO 4/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley del Impuesto sobre Sociedades.
- RESOLUCIÓN de 23 de diciembre de 2009, de la Dirección General de Planificación, Ordenación e Inspección Educativa, por la que se concreta la gestión de los procesos de admisión y matriculación del alumnado en centros docentes sostenidos con fondos públicos que impartan enseñanzas de segundo ciclo de Educación Infantil, Educación Primaria, Educación Secundaria Obligatoria y Bachillerato de la Comunidad de Castilla y León, para el curso 2010/2011.

**Páginas Web visitadas**

- www.davara.net
- www.davara.com
- www.ubu.es
- http://gicap.ubu.es/MAC-TIC/
- www.boe.es
- www.bocyl.es
- www.jcyl.es
- https://www.agpd.es/portalwebAGPD/index-ides-idphp.php
- http://noticias.juridicas.com/
- http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html
- http://www.educacion.es/portada.html
- http://red.es/index.action
- http://www.icann.org/en/announcements/
- http://www.meh.es/es-ES/Paginas/Home.aspx
- http://www.mityc.es/es-ES/Paginas/index.aspx
- http://europa.eu/index_es.htm
- http://www.samuelparra.com/
- http://www.fnmt.es/

- http://www.mityc.es/dgdsi/lssi/normativa/Paginas/normativa.aspx
- http://www.nic.es/resoluciones-dictadas/article/1485
- http://civil.udg.es/normacivil/estatal/reals/Lpi.html
- http://impuestosrenta.com/ley-iva/
- http://www.wipo.int/amc/es/docs/icannpolicy.pdf
- www.ine.es