



UNIVERSIDAD DE ALMERÍA

Manual de usuario en materia de protección de datos de carácter personal de la entidad

**Universidad de Almería.**

**ADAPTADO AL REAL DECRETO 1720/2007**

Mayo de 2011

## Índice

1. Introducción .....	1
2. Glosario de términos básicos .....	2
3. Niveles de seguridad de los datos .....	5
4. Funciones y obligaciones de los usuarios .....	7
5. Gestión de incidencias .....	11
5.1. Procedimiento para la gestión de incidencias relativas a ficheros automatizados .....	12
5.2. Procedimiento para la gestión de incidencias relativas a ficheros no automatizados .....	12
6. Ejercicio de derechos .....	14
7. Procedimiento para el uso del correo electrónico y en general de las TIC .....	16
8. Procedimiento para los envíos telemáticos .....	17
9. Procedimiento de registro de entrada de soportes .....	19
10. Procedimiento de registro de salida de soportes .....	20
11. Procedimiento de desechado y reutilización de soportes automatizados .....	21
12. Procedimiento de desechado y reutilización de soportes no automatizados .....	22
13. Procedimiento de custodia de soportes no automatizados .....	23
14. Procedimiento de archivo de ficheros no automatizados .....	24
15. Procedimiento de restricción de acceso a ficheros no automatizados .....	25
16. Procedimiento de copia y reproducción de documentos .....	26
17. Procedimiento de traslado de documentación .....	27
18. Responsables de seguridad .....	28

## 1. Introducción

La protección de los datos de carácter personal de los ciudadanos ha sido regulada por el legislador español mediante la L.O. 15/1999 (LOPD) y una serie de normas que la desarrollan y complementan, que establecen toda una serie de medidas de obligado cumplimiento para aquellas entidades que, en el ejercicio de su actividad, sometan a tratamiento este tipo de datos de carácter personal.

El RD 1720/2007, Reglamento de desarrollo de la LOPD, o RDLOPD), desarrolla los principios y obligaciones dispuestos en la LOPD.

La LOPD y el RDLOPD, cuyo objeto principal lo constituye la salvaguarda del derecho al honor, la intimidad personal, y la propia imagen de las personas físicas, atribuyen determinadas funciones y obligaciones a todas aquellas personas que intervienen en el tratamiento de los ficheros donde se almacenan los datos de carácter personal.

La Ley impone sanciones económicas muy elevadas a las organizaciones privadas (sanciones que pueden llegar - sólo por una infracción - hasta los 600.000 euros) y sanciones no económicas pero si de otra índole (publicidad de la sanción, inmovilización temporal del fichero, etc...) a las organizaciones públicas.

Es, por tanto, objeto de este manual el detallar las funciones y obligaciones que, como usuario de los ficheros con datos de carácter personal de la entidad, le corresponde conocer y respetar.

## 2. Glosario de términos básicos

**DATOS DE CARÁCTER PERSONAL:** cualquier información concerniente a personas físicas identificadas o identificables.

Es decir, cualquier dato que podamos relacionar con personas físicas. En el ámbito de las empresas esas personas serán normalmente potenciales clientes, clientes, proveedores, trabajadores de la empresa, terceros o personas de contacto. En algunos ámbitos concretos de actividad puede que los datos se refieran a otras personas como pacientes, asociados ... o por ejemplo en el ámbito público dichos afectados son los ciudadanos, contribuyentes etc., además de algunos afectados comunes al ámbito privado: por ejemplo los empleados, proveedores, contactos, etc...

Téngase en cuenta que no sólo se refiere a personas identificadas (cuando tengamos su nombre) sino también cuando esas personas sean razonablemente identificables por ejemplo a través de un identificador: por ejemplo número de colegiado, DNI, IP, correo electrónico etc...

**AFECTADO O INTERESADO:** persona física titular de los datos.

Es la persona cuyos datos se tratan, es decir: el cliente, paciente, ciudadano, empleado, proveedor, contacto, etc...

**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.

Téngase en cuenta que a tenor de la definición de tratamiento que da la Ley cualquier operación que se haga con ellos: grabarlos, modificarlos, conservarlos, enviarlos, etc... constituirá tratamiento.

**FICHERO:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Es decir, cualquier dato que tengamos sobre personas físicas en cualquier tipo de soporte, tanto papel como a nivel informático.

El concepto de fichero no se corresponde necesariamente con una base de datos, sino que siempre que exista un conjunto de datos que estén organizados mediante algún criterio, nos encontraremos ante la existencia de un fichero. Obviamente una aplicación informática de nóminas constituye un ejemplo de fichero, pero también lo puede constituir una tabla de datos en Word, sin olvidar que también es aplicable este concepto a los datos no automatizados: por ejemplo un archivo A-Z.

**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.

El responsable del fichero normalmente coincidirá con la organización: la empresa, asociación, institución, empresarios individual, profesional, etc... y es a quien se le imponen la mayoría de las obligaciones en protección de datos siendo, por tanto, normalmente el responsable de las sanciones que - en su caso - se impongan. Ello sin perjuicio de que el responsable del fichero pueda nombrar una persona física que le represente.

**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.

El encargado del tratamiento es un tercero (normalmente una empresa pero no necesariamente) que le presta un servicio al responsable del fichero y que para ello requiere acceder a datos del responsable. Ejemplos típicos de encargados lo son la asesoría laboral, contable o fiscal (que acceden a los datos de empleados, clientes o proveedores de su cliente para asesorarle), empresas de mantenimiento de hardware o software, etc... El servicio que presta el encargado no tiene porqué ser remunerado. La relación entre el responsable y el encargado se debe regular mediante un contrato cuyo contenido establece el artículo 12 de la LOPD.

**USUARIOS:** sujeto o proceso autorizado a acceder a datos o recursos.

Normalmente un usuario será una persona que accede a datos de la organización. El usuario podrá tener diferentes perfiles de acceso y ser un usuario interno o externo (un usuario de otra organización que accede a nuestro sistema para prestar un servicio, por ejemplo mantenimiento informático).

**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.

El responsable de seguridad puede ser uno o varios y son los 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, que es a quien en primera instancia se le pueden imponer en su caso las sanciones que contempla la Ley. Ello es sin perjuicio de que el responsable de seguridad si no cumple con sus obligaciones pueda tener responsabilidad laboral o disciplinaria.

**CONSENTIMIENTO:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Téngase en cuenta que el consentimiento es el eje vertebral de la protección de datos y ello exige que como regla general no se puedan tratar datos de nadie sin consentimiento, sin perjuicio de que en ocasiones esta obligación está exenta. Por ejemplo: cuando los datos se traten en el marco de la relación comercial, laboral o administrativa, cuando exista una Ley que disponga lo contrario, etc...

**COMUNICACIÓN DE DATOS:** Toda revelación de datos realizada a una persona distinta del interesado.

La cesión de datos debe estar, salvo excepciones, necesariamente consentida por el interesado. Por ello, es importante no comunicar datos de carácter personal a otras personas físicas o jurídicas, salvo que se disponga del consentimiento de dicha persona o se esté ante alguna de las excepciones previstas por la Ley.

### 3. Niveles de seguridad de los datos

Las medidas de seguridad que dispone el RDLOPD se dividen en tres niveles, según la sensibilidad de los datos que se contienen en los ficheros: nivel básico, medio y alto. Las medidas se aplican de modo acumulativo.

Tenga en cuenta que deberán cumplirse - como mínimo - las medidas correspondientes al nivel del fichero. Sin embargo, el Responsable de Seguridad podrá implementar medidas de nivel superior cuando así considere oportuno.

NIVEL	DESCRIPCIÓN
Básico	- Todos
Medio	<ul style="list-style-type: none"> <li>- Los relativos a la comisión de infracciones administrativas o penales.</li> <li>- Los relativos al art. 29 LOPD (ficheros de solvencia patrimonial y crédito).</li> <li>- Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.</li> <li>- Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.</li> <li>- Aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.</li> <li>- Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.</li> <li>- Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.</li> </ul>

<p>Alto</p>	<ul style="list-style-type: none"> <li>- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.</li> <li>- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.</li> <li>- Aquellos que contengan datos derivados de actos de violencia de género.</li> </ul>
<p>EXCEPCIONES</p>	<ul style="list-style-type: none"> <li>- A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento (registro de accesos).</li> <li>- En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:             <ul style="list-style-type: none"> <li>\na) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.</li> <li>\nb) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesorio se contengan aquellos datos sin guardar relación con su finalidad.</li> </ul> </li> <li>- También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.</li> </ul>

## 4. Funciones y obligaciones de los usuarios

El personal que, para el correcto desarrollo de su labor, tiene autorizado acceso a datos personales, tiene las siguientes obligaciones:

### **CON RESPECTO A FICHEROS AUTOMATIZADOS**

#### 1. OBLIGACIONES GENERALES

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

2. Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

3. Queda prohibido el traslado de cualquier soporte, listado o documento con datos de carácter personal en los que se almacene información titularidad de la organización fuera de los locales de la misma, sin autorización previa del Responsable de Seguridad. En el supuesto de existir traslado o distribución de soportes y documentos se realizará cifrando dichos datos, o mediante otro mecanismo que impida el acceso o manipulación de la información por terceros.

4. Ficheros de carácter temporal o copias de documentos son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada o trabajos temporales y auxiliares, siempre y cuando su existencia no sea superior a un mes. Estos ficheros de carácter temporal o copias de documentos deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán cumplir con los niveles de seguridad asignados por el Responsable de Seguridad.

Si, transcurrido el mes, el usuario necesita continuar utilizando la información almacenada en el fichero, deberá comunicarlo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.

5. Únicamente las personas autorizadas en un listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros o documentos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable de Seguridad correspondiente.

6. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

## 2. OBLIGACIONES RESPECTO DE LOS FICHEROS AUTOMATIZADOS

1. Cambiar las contraseñas a petición del sistema.
  2. Cerrar o bloquear todas las sesiones al término de la jornada laboral o en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.
  3. No copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal al ordenador personal, disquetes, portátil o a cualquier otro soporte sin autorización expresa del Responsable de Seguridad correspondiente.
  4. Guardar todos los ficheros con datos de carácter personal en la carpeta indicada por el Responsable de Seguridad correspondiente, a fin de facilitar la aplicación de las medidas de seguridad que les correspondan.
  5. Los usuarios tiene prohibido el envío de información de carácter personal de nivel alto, salvo autorización expresa del Responsable de Seguridad que tenga asignada esta tarea. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.
  6. Los usuarios no podrán, salvo autorización expresa del Responsable de Seguridad que tenga asignada esta tarea, instalar cualquier tipo de programas informáticos o dispositivos ni en los servidores centrales ni en el ordenador empleado en el puesto de trabajo.
7. Queda prohibido:
- a. Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.
  - b. Intentar modificar o acceder al registro de accesos habilitado por el Responsable de Seguridad competente.
  - c. Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.
  - d. Enviar correos masivos (spam) empleando la dirección de correo electrónico corporativa.
  - e. Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

Estas obligaciones sólo serán exigibles a los usuarios de ficheros automatizados, en tanto en cuanto la organización disponga los medios adecuados en cada caso.

***Ficheros afectados***

- EXPEDIENTES ACADÉMICOS ALUMNOS

**CON RESPECTO A FICHEROS NO AUTOMATIZADOS**

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la entidad.
2. Mantener debidamente custodiadas las llaves de acceso a la residencia, a sus despachos y a los armarios, archivadores u otros elementos que contenga ficheros no automatizados con datos de carácter personal, debiendo poner en conocimiento del Responsable de Seguridad cualquier hecho que pueda haber comprometido esa custodia.
3. Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
4. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.
5. Queda prohibido el traslado de cualquier listado o documento análogo con datos de carácter personal en los que se almacene información titularidad de la entidad fuera de los locales de la misma.
6. Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.
7. Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.
8. Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros objeto de protección. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable de Seguridad.
9. Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada, siempre y cuando su existencia no sea superior a un mes. Los ficheros de carácter

temporal deben ser destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán contemplarse las medidas de seguridad contenidas en este documento.

***Ficheros afectados***

- EXPEDIENTES ACADÉMICOS ALUMNOS

## 5. Gestión de incidencias

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

En caso de conocer alguna incidencia ocurrida, el usuario debe comunicarla al responsable de seguridad competente que adoptará las medidas oportunas.

Las incidencias pueden afectar tanto a ficheros automatizados como no automatizados.

Ejemplos de incidencias comunes que pudieran afectar a los datos personales contenidos en ficheros automatizados son las siguientes:

- Alteración en los permisos, altas o bajas de usuarios.
- Olvido de contraseña.
- Bloqueo de cuenta por reiteración de intentos de conexión fallidos.
- Pérdida de datos.

Por su parte algunos ejemplos de incidencias que pueden afectar a ficheros no automatizados son los siguientes:

- Robo o pérdida de llaves de lugares o soportes en donde se almacenen dichos ficheros no automatizados.
- Desaparición de documentos o soportes que contengan datos personales.

No obstante dicha relación no es taxativa y debe comunicar al responsable de seguridad cualquier incidencia que afecte a los datos de carácter personal.

El concreto procedimiento/s de gestión de incidencias implantado/s en la organización es/son el siguiente/s:

### 5.1. Procedimiento para la gestión de incidencias relativas a ficheros automatizados

El procedimiento de notificación y gestión de incidencias relativo a ficheros automatizados al que se refiere el presente documento consiste en:

La gestión de notificación de incidencias se notificará a través de un enlace de una cuenta de correo electrónico (incidencias.lopdp@ual.es) en la página web de la comisión de Seguridad informática.

Dicho correo será gestionado por el personal competente que gestionará las incidencias y llevará un registro de las mismas.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

No obstante y sin perjuicio de que en el último apartado se designan el/los responsable/s de seguridad a quien ha de dirigirse, en concreto el responsable de seguridad designado para la gestión de incidencias para ficheros automatizados es:

**Diego Pérez**

### 5.2. Procedimiento para la gestión de incidencias relativas a ficheros no automatizados

El procedimiento de notificación y gestión de incidencias relativo a ficheros no automatizados al que se refiere el presente documento consiste en:

La gestión de notificación de incidencias se notificará a través de un enlace de una cuenta de correo electrónico (incidencias.lopdp@ual.es) en la página web de la comisión de Seguridad informática.

Dicho correo será gestionado por el personal competente que gestionará las incidencias y llevará un registro de las mismas.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

No obstante y sin perjuicio de que en el último apartado se designan el/los responsable/s de seguridad a quien ha de dirigirse, en concreto el responsable de

seguridad designado para la gestión de incidencias para ficheros no automatizados es:

**Carmen Alicia García**

## 6. Ejercicio de derechos

La legislación sobre protección de datos otorga a los interesados una serie de derechos que estos podrán ejercitar en relación con sus datos personales. Estos derechos son el derecho de acceso, rectificación, oposición y cancelación, en relación con sus datos personales.

Normalmente en las organizaciones existen unos usuarios (a los que denominamos usuarios de atención) que son los encargados de recoger estas peticiones (normalmente en las empresa los servicios de atención al cliente, o en las organizaciones públicas los servicios de atención al ciudadano o quienes se hayan en los registros). No obstante tenga en cuenta que caso de que usted reciba una consulta verbal o petición de ejercicio de derechos deberá actuar siguiendo el procedimiento establecido por la organización:

El procedimiento de gestión y resolución de ejercicios de derecho consiste en:

1. Ante la consulta (por ejemplo llamada) sobre algún ejercicio de derechos por parte de algún interesado.: - Dar información sobre en qué consiste el Derecho, plazos etc... Es decir sobre el procedimiento. - No ofrecerle datos sobre la persona, sobre el fondo del asunto etc. - Tomar nota (sólo tomar nota) de la persona de que se trata (de su identidad) y del motivo. - Hacerle llegar (si lo pide) el impreso correspondiente para ejercitar el derecho por una vía que permita dejar constancia (reporte de fax o copia email).
2. Ante la recepción de alguna petición de ejercicio de derechos (normalmente por carta, fax o email): - Si dispone del módulo de ejercicio de derechos de GESDATOS: introducir la solicitud en la herramienta. - Si no dispone del módulo de ejercicio de derechos de GESDATOS: remitir la solicitud inmediatamente al responsable de seguridad que tenga atribuida esta tarea.
3. Ante cualquier otra cuestión en esta materia.: - Acudir al responsable de seguridad que tenga atribuida esta tarea.

### *Ficheros afectados*

- EXPEDIENTES ACADÉMICOS ALUMNOS
- EXPEDIENTES ACADÉMICOS ALUMNOS

*Documentación adicional*

Adicionalmente a la información aquí descrita, se encuentran disponibles los siguientes documentos ubicados en las siguientes URLs:

-

<http://cms.ual.es/UAL/universidad/otrosorganos/comisionseguridad/derechos/index.htm> : Derechos de los Titulares de los Datos Personales

No obstante y sin perjuicio de que en el último apartado se designan el/los responsable/s de seguridad a quien ha de dirigirse, en concreto el responsable de seguridad designado para la resolución de las peticiones de ejercicio de derechos es:

**M<sup>a</sup> Ángeles Piedra**

## 7. Procedimiento para el uso del correo electrónico y en general de las TIC

La organización puede definir una política de uso y control del correo electrónico, y también - en general - de uso y control de las TIC.

En caso de que la organización haya definido una política de uso y control del correo, o más genérica de las TIC, la misma debe ser conocida por los usuarios. Por ello - caso de haberse adoptado - se detalla a continuación. Como usuario deberá conocerla y cumplirla.

El procedimiento de uso y control del email y las TIC de la organización es el siguiente:

La normativa de uso del correo electrónico se detalla en el documento del hipervínculo.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

### *Documentación adicional*

Adicionalmente a la información aquí descrita, se encuentran disponibles los siguientes documentos ubicados en las siguientes URLs:

-

[http://cms.ual.es/idc/groups/public/@otros/@comisionseguridad/documents/documento/politica\\_seguridad\\_ual.pdf](http://cms.ual.es/idc/groups/public/@otros/@comisionseguridad/documents/documento/politica_seguridad_ual.pdf) : Política de seguridad de la UAL. (aprobada el 2-may-2006)

## 8. Procedimiento para los envíos telemáticos

El RDLOPD, para los ficheros de nivel alto, obliga al cifrado de datos o la utilización de cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros, cuando los mismos vayan a ser objeto de transmisión a través de redes públicas o redes inalámbricas.

En caso de que la organización haya definido un procedimiento para los envíos telemáticos de nivel alto la misma se detalla a continuación. Como usuario deberá conocerla y cumplirla.

El procedimiento de envíos telemáticos al que se refiere el presente documento consiste en:

El RDLOPD, para los ficheros de nivel alto, obliga al cifrado de datos o la utilización de cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros, cuando los mismos vayan a ser objeto de transmisión a través de redes de telecomunicaciones.

El envío de datos a través de redes de telecomunicaciones supone la adopción de una serie de medidas organizativas y técnicas que se han de respetar y constituyen el procedimiento a seguir. Este procedimiento afecta a diversos niveles:

1) A nivel organizativo:

a) Los usuarios deben conocer (y así se debe reflejar en su manual y/o en las normas usuario del sistema de información) las pautas a seguir al respecto.

b) El usuario deberá contar con la autorización del Responsable del Fichero o del Responsable de Seguridad, que tenga atribuidas estas funciones por delegación.

2) A nivel técnico, el Usuario, bien por su propia cuenta, mediante los mecanismos que se hubieran puesto a disposición o bien, por parte del Responsable de Seguridad y/o técnico informático, debe proceder al cifrado de los datos o la utilización de cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Los envíos telemáticos de becas al Ministerio se realizan a través de un Web Service, comprimido en Zip y encriptado con 64 bits.

***Ficheros afectados***

- EXPEDIENTES ACADÉMICOS ALUMNOS

## 9. Procedimiento de registro de entrada de soportes

El RDLOPD obliga a la adopción de determinadas medidas para garantizar la seguridad de los datos que entran o salen de las organizaciones.

En el caso de entradas de soportes deberá disponerse de un sistema de registro de entrada de soportes que contenga la información dispuesta reglamentariamente.

Tenga en cuenta que ellos es importante porque, especialmente las salidas de soportes y documentos, constituyen un hecho que puede ser crítico ya que en muchas ocasiones las mismas se realizan sin respetar las obligaciones tanto jurídicas como técnicas dispuestas legalmente y suponen en ocasiones el acceso por parte de terceros a información que no deben conocer. Por tanto ante una entrada o salida de documentos o soportes que contengan ficheros con datos personales deberá dirigirse al responsable de seguridad competente que le informará de la forma de proceder.

El procedimiento de entrada de soportes y documentos a los que se refiere el presente documento es el siguiente:

Las entradas de soportes que contengan datos personales, cuyo nivel de seguridad sea como mínimo de nivel medio, deberán ser registradas en el registro de GESDATOS que contiene la siguiente información: el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

### *Ficheros afectados*

- EXPEDIENTES ACADÉMICOS ALUMNOS
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 10. Procedimiento de registro de salida de soportes

El RDLOPD obliga a la adopción de determinadas medidas para garantizar la seguridad de los datos que entran o salen de las organizaciones.

En el caso de salidas de soportes deberá disponerse de un sistema de registro de salida de soportes que contenga la información dispuesta reglamentariamente.

Adicionalmente las salidas de soportes deben estar autorizadas por el responsable de seguridad competente.

Tenga en cuenta que ellos es importante porque, especialmente las salidas de soportes y documentos, constituyen un hecho que puede ser crítico ya que en muchas ocasiones las mismas se realizan sin respetar las obligaciones tanto jurídicas como técnicas dispuestas legalmente y suponen en ocasiones el acceso por parte de terceros a información que no deben conocer. Por tanto ante una entrada o salida de documentos o soportes que contengan ficheros con datos personales deberá dirigirse al responsable de seguridad competente que le informará de la forma de proceder.

El procedimiento de salida de soportes y documentos a los que se refiere el presente documento es el siguiente:

Las salidas de soportes que contengan datos personales, como mínimo de nivel medio, deberán ser registradas en el registro de GESDATOS que contiene la siguiente información: el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

### *Ficheros afectados*

- EXPEDIENTES ACADÉMICOS ALUMNOS
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 11. Procedimiento de desechado y reutilización de soportes automatizados

El desechado y/o reutilización de soportes y documentos que contienen datos personales, tanto en ficheros automatizados como no automatizados, pueden suponer el acceso indebido por parte de terceros a los datos personales que se contienen en los mismos si no se realiza de forma correcta.

La organización debe de disponer de un procedimiento que detalle la forma de proceder en estos casos.

En el caso de soportes automatizados (medida a adoptar para TODOS LOS NIVELES) siempre que vaya a desecharse cualquier soporte automatizado que contenga datos de carácter personal (cualquiera que sea su nivel) deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. También deberá procederse al borrado de la documentación cuando el soporte vaya a reutilizarse.

En caso de que la organización haya definido un procedimiento para el desechado o reutilización de soportes automatizados el mismo se detalla a continuación. Como usuario deberá conocerlo y cumplirlo.

El procedimiento de desechado o reutilización de soportes para ficheros automatizados consiste en:

El procedimiento de reutilización de soportes consiste en el formateado previo del dispositivo si éste lo permite, para su posterior reutilización.

En el caso de proceder a la destrucción del soporte (siempre que se procede a su destrucción es porque el soporte ha dado error), se procederá a su destrucción física.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 12. Procedimiento de desechado y reutilización de soportes no automatizados

El desechado y/o reutilización de soportes y documentos que contienen datos personales, tanto en ficheros automatizados como no automatizados, pueden suponer el acceso indebido por parte de terceros a los datos personales que se contienen en los mismos si no se realiza de forma correcta.

La organización debe de disponer de un procedimiento que detalle la forma de proceder en estos casos.

En el caso de soportes no automatizados (medida que se ciñe al NIVEL ALTO, pero que se puede ampliar si así se indica en el procedimiento a otros niveles) deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

En caso de que la organización haya definido un procedimiento para el desechado de soportes no automatizados el mismo se detalla a continuación. Como usuario deberá conocerlo y cumplirlo.

El procedimiento de desechado o reutilización de soportes para ficheros no automatizados consiste en:

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. Las medidas a aplicar serán:

En el caso de que se trate de documento en papel, cuando éstos contengan datos de carácter personal, queda prohibida su reutilización (a modo de papel reciclado). En todo caso, se procederá a su destrucción mediante el uso de la destructora de papel. Para la destrucción de un gran volumen de información se contratan los servicios de una empresa de destrucción confidencial.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 13. Procedimiento de custodia de soportes no automatizados

El procedimiento de custodia de la organización es el siguiente:

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal disponen de mecanismos que obstaculizan su apertura. En el documento de seguridad se relaciona el mecanismo que obstaculiza la apertura en relación con cada soporte.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 14. Procedimiento de archivo de ficheros no automatizados

El procedimiento de archivo es el siguiente:

El archivo de los soportes se realiza siguiendo un criterio funcional, según un cuadro de clasificación, que permite su localización visual. Debido a su poco volumen no se dispone de un registro informático de localización.

Debido al volumen de soportes existentes se dispone de un registro informático que posibilita su localización.

Adicionalmente y debido al volumen de archivos, una vez los soportes han permanecido durante su vida útil en el archivo vivo pasan al archivo histórico.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 15. Procedimiento de restricción de acceso a ficheros no automatizados

El procedimiento de ubicación de áreas restringidas de la organización es el siguiente:

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.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 16. Procedimiento de copia y reproducción de documentos

El RDLOPD dispone que en el caso de ficheros no automatizados que contengan datos de nivel alto las copias o reproducciones únicamente podrán ser realizadas bajo el control del personal autorizado en el documento de seguridad.

En caso de que la organización haya definido un procedimiento para la copia o reproducción de documentos el mismo se detalla a continuación. Como usuario deberá conocerlo y cumplirlo.

El procedimiento de copia y reproducción de documentos de la organización es el siguiente:

La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad. La reproducción de copias se realiza mediante petición formal escrita al personal competente en la materia (personal de archivo), según legislación vigente en la materia.

Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 17. Procedimiento de traslado de documentación

El RDLOPD obliga a adoptar ciertas medidas dirigidas a proteger la información contenida en ficheros no automatizados que sea objeto de traslado, cuando los mismos contengan información de nivel alto.

En caso de que la organización haya definido dichas medidas para proceder al traslado de documentación de nivel alto (obligación que podrá ampliarse a cualquier otro nivel de datos si así se indica) las mismas se detallan a continuación. Como usuario deberá conocerlas y cumplirlas.

El procedimiento de traslado de documentación de la organización es el siguiente:

### TRASLADO DE DOCUMENTACIÓN PARA FICHEROS DE NIVEL ALTO

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

<i>Ficheros afectados</i>
- EXPEDIENTES ACADÉMICOS ALUMNOS

## 18. Responsables de seguridad

El Responsable/s de seguridad es el encargado/s de autorizar, coordinar, controlar y en algunos casos ejecutar las medidas de seguridad dispuestas en materia de protección de datos.

Tenga en cuenta que estas personas son muy importantes en el funcionamiento de un sistema de protección de datos y que ante cualquier duda o cuestión en materia de protección de datos deberá dirigirse a el/ellos. En el caso de que existan varios tenga en cuenta que tendrán las tareas divididas.

Los responsables de seguridad designados por la organización son los siguientes:

<b>Nombre y Apellidos</b>	<b>Email</b>	<b>Departamento</b>
<b>Carmen Alicia García</b>		<b>Archivo y documentación</b>
<b>Diego Pérez</b>		<b>STIC</b>
<b>M<sup>a</sup> Ángeles Piedra</b>		<b>Departamento jurídico</b>