



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

MANUAL DE PROTECCIÓN DE DATOS
DE CARÁCTER PERSONAL
Universidad Politécnica de Valencia



ÁREA DE SISTEMAS
DE INFORMACIÓN
Y COMUNICACIONES

Febrero 2005

0. Contenido.

1. Objetivo y ámbito de aplicación.

2. Los Datos de Carácter Personal en la UPV.

- 2.1 ¿Qué son datos de carácter personal?. Tipos de datos y ficheros.
- 2.2 Ley Orgánica de Protección de Datos de Carácter Personal.
- 2.3 Disociación de los datos.
- 2.4 Política general de protección de datos de carácter personal UPV.

3. Notificación de los ficheros.

- 3.1 ¿Quién debe notificar?.
- 3.2 Notificación e inscripción de un fichero.
- 3.3 Responsable del Fichero.
- 3.4 Tipo de los datos.
- 3.5 Finalidad y usos del fichero.
- 3.6 Cesiones de datos.

4. Legalización de los ficheros.

- 4.1 Información previa al interesado.
- 4.2 Consentimiento del interesado.
- 4.3 Calidad de los datos.
- 4.4 Deber de secreto.
- 4.5 Comunicación de datos personales. Cesiones.
- 4.6 Prestaciones de servicio.
- 4.7 Derechos de los afectados.
 - 4.7.1 Procedimiento ante peticiones de acceso, rectificación, cancelación y oposición a los datos personales.
 - 4.7.2 Derecho de acceso.
 - 4.7.3 Derecho de rectificación.
 - 4.7.4 Derecho de cancelación.
 - 4.7.5 Derecho de oposición.

5. Notificación, gestión y respuesta ante incidencias.

- 5.1. Notificación, gestión y respuesta ante Incidencias.
- 5.2. Procedimiento de Registro de Incidencias.
- 5.3. Procedimiento de Notificación de Incidencias.
- 5.4. Modelo de Comunicación de Incidencias.

6. Protección de los ficheros. Reglamento de Seguridad.

- 6.1 Reglamento de Medidas de Seguridad.
- 6.2 El Documento de Seguridad.

ANEXO 1. Regulación de los ficheros automatizados de datos de carácter personal de la UPV.

ANEXO 2. Modelo normalizado para la declaración ante la AEPD de ficheros con datos de carácter personal.

ANEXO 3. Modelo de resolución de creación, modificación o supresión de fichero a insertar en el DOGV.

ANEXO 4. Modelo de contrato para prestaciones de servicios.

ANEXO 5. Modelos de solicitudes para el ejercicio de los derechos de los interesados.

ANEXO 6. Legislación aplicable e instrucciones AEPD.

- Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD).
- R.D. 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.
- Instrucciones AEPD.

ANEXO 7. Preguntas más frecuentes.

- Ficheros en soporte papel o ficheros manual-estructurados.

ANEXO 8. Comunicaciones internas sobre protección de datos personales.

1. Objetivo y Ámbito de Aplicación.

El presente Manual de Protección de Datos de Carácter Personal de la Universidad Politécnica de Valencia (UPV) recoge un resumen de la política, normas, reglas, estándares, procedimientos y otras consideraciones a tener en cuenta en el manejo de los datos de carácter personal contenidos en los ficheros de la UPV.

Las normas, procedimientos y recomendaciones expresadas en este manual se aplicarán a todos los ficheros de datos de carácter personal existentes en la UPV. Los ficheros automatizados de datos de carácter personal de la Universidad Politécnica de Valencia son los que se relacionan y regulan en el **Anexo 1** del presente documento (***Regulación de los ficheros automatizados de datos de carácter personal de la UPV***).

No pueden existir ficheros con datos personales distintos de los que figuran en el **Anexo 1**, los cuales han sido debidamente autorizados y declarados a la Agencia Española de Protección de Datos (AEPD). Si fuera necesaria la creación de un fichero nuevo que contenga datos de carácter personal, se deberá seguir previamente el procedimiento establecido en este manual para dar de alta el fichero en la AEPD y será incluido el fichero en el documento de *Regulación de los ficheros automatizados de datos de carácter personal de la UPV*.

2. Los Datos de Carácter Personal en la UPV.

- 2.1 ¿Qué son datos de carácter personal?. Tipos de datos y ficheros.
 - 2.2 Ley Orgánica de Protección de Datos de Carácter Personal.
 - 2.3 Disociación de los datos.
 - 2.4 Política general de protección de datos de carácter personal UPV.
-

2.1. ¿Qué son datos de carácter personal?. Tipos de datos y ficheros.

Son **datos de carácter personal** toda información concerniente a personas físicas identificadas o identificables (nombre, edad, sexo, estado civil, domicilio, etc), que aparece registrada en cualquier soporte físico (ficheros) que permita su tratamiento manual o automatizado y posterior uso por el sector público o privado. Es conveniente destacar que la Agencia Española de Protección de Datos mantiene que el correo electrónico son también datos personales ya que permite identificar a la persona.

Un **fichero** es un conjunto organizado de datos de carácter personal, cualquiera que sea la forma y modalidad de su creación, almacenamiento, organización y acceso. Hay que tener en cuenta que dentro del concepto de fichero se incluyen tanto los ficheros automatizados (cualquier base de datos) como los ficheros manuales.

Atendiendo a la titularidad de los ficheros de datos, éstos pueden clasificarse en ficheros de titularidad pública y ficheros de titularidad privada.

- a) Los **ficheros de titularidad pública** son los que crean las Administraciones Públicas en el ejercicio de sus funciones. Su creación requiere una disposición general publicada en el B.O.E. o en el diario oficial correspondiente.
- b) Los **ficheros de titularidad privada** son los que cualquier particular o empresa privada crea para el desarrollo de actividades legítimas.

Atendiendo a la forma de organizar el fichero, se distingue entre ficheros automatizados y ficheros manuales.

- a) Los **ficheros automatizados** son las bases de datos o cualquier otra forma de almacenamiento organizado de la información a las que se incorporan datos de carácter personal.
- b) Los **ficheros manuales** son el resto de ficheros que no están soportados por medios automáticos para el almacenamiento y el tratamiento de los datos.

2.2. Ley Orgánica de Protección de Datos de Carácter Personal.

La Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) (**ANEXO 6**), y el R.D. 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 (Reglamento) (**ANEXO 6**), son las dos disposiciones básicas de obligado cumplimiento para todas las organizaciones y profesionales que, en el desarrollo de su actividad, traten datos de carácter personal.

La LOPD establece una serie de obligaciones relativas a la recogida de los datos, consentimiento, almacenaje, conservación, uso, datos especialmente protegidos, comunicación o cesión de datos, acceso, rectificación, creación de ficheros, alta en el Registro de la Agencia Española de Protección de Datos, etc.

La LOPD es aplicable a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Están excluidos del ámbito de la LOPD los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas (por ej. una agenda personal no es un fichero sometido a la LOPD).

Por su parte, el Reglamento establece las medidas que se han de adoptar obligatoriamente para garantizar la seguridad respecto de los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

Las obligaciones legales pueden resumirse en cuatro partes:

- a) **Notificación de los ficheros** de datos a la Agencia Española de Protección de Datos.
- b) **Adopción de las medidas de seguridad** relacionadas en la LOPD y el Reglamento en función del nivel de seguridad exigible.
- c) **Redacción del documento de seguridad** que recoja todas las medidas adoptadas.
- d) **Redacción de los contratos y aplicación de las cláusulas** necesarias para la recogida de datos, los tratamientos por terceros y las cesiones o comunicaciones de datos.

2.3. Disociación de los datos.

La LOPD define el procedimiento de disociación como *“todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable”*.

Es recomendable aplicar técnicas de disociación en todos aquellos procedimientos que lo permitan para evitar que los datos identifiquen a personas físicas. De esta forma los datos dejan de ser de carácter personal y no es necesario contemplar todas las garantías que exige la LOPD.

2.4. Política general de protección de datos de carácter personal UPV.

La Universidad Politécnica de Valencia tiene como preocupación fundamental garantizar la privacidad e integridad de los datos de carácter personal de los miembros de su comunidad y, en general, de todos los usuarios de los sistemas de información de la institución, y con esta finalidad se deben adoptar las medidas técnicas y organizativas necesarias para protegerlos.

Los datos personales recogidos, ya sea por medios telemáticos o por cualquier otro medio, no se utilizarán para ninguna otra finalidad que no sea la relacionada con las actividades propias de la Universidad y que han sido declaradas para cada fichero a la Agencia Española de Protección de Datos.

En la práctica deberá haber separación de funciones y revisión independiente de las operaciones o transacciones realizadas cuando sea necesario, a partir de los registros, de quién ha hecho qué, cuándo y desde dónde.

Cada función sólo podrá realizar las tareas y acceder a los datos necesarios que se requieran para cumplir su cometido, es decir se considerará el principio del llamado "mínimo privilegio" para evitar accesos no autorizados.

Se designará internamente al **responsable propietario de cada fichero** o base de datos, que será quien deberá promover el establecimiento de controles y medidas tendentes a proteger los datos bajo su responsabilidad.

En previsión de la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar la posible existencia de anomalías lo antes posible, se fomentará la difusión de información y se promoverá la formación en seguridad entre empleados y colaboradores.

3. Notificación de los ficheros.

- 3.1 ¿Quién debe notificar?.
 - 3.2 Notificación e inscripción de un fichero.
 - 3.3 Responsable del Fichero.
 - 3.4 Tipo de los datos.
 - 3.5 Finalidad y usos del fichero.
 - 3.6 Cesiones de datos.
-

3.1. ¿Quién debe notificar?.

Cualquier persona o entidad que pretenda crear un fichero que contenga datos de carácter personal, debe notificarlo a la Agencia Española de Protección de Datos (AEPD) **con carácter previo** a la creación del fichero de que se trate, a fin de que la Agencia proceda a inscribirlo en el Registro General de Protección de Datos. La obligación de notificación recae en el **Responsable del Fichero**.

Una vez notificado e inscrito un fichero, el Responsable del Fichero está también **obligado a notificar** a la AEPD los **cambios** que se produzcan en el fichero o la baja del mismo.

3.2. Notificación e inscripción de un fichero.

El Responsable del Fichero procederá a su notificación mediante el **modelo normalizado (ANEXO 2)** que se remitirá al Área de Sistemas de Información y Comunicaciones (ASIC) para que desde allí se gestione su envío a la AEPD para su inscripción en el Registro General de Protección de Datos.

Asimismo, el Responsable del Fichero remitirá al ASIC la resolución de creación, modificación o supresión del fichero (según modelo del **ANEXO 3**) que es necesario publicar en el DOGV antes de la notificación a la AEPD. El ASIC gestionará la publicación de dicha inscripción en el DOGV. Una vez publicada la resolución, se tramitará la inscripción con la AEPD y se notificará al responsable propietario del fichero sobre la inscripción del fichero una vez se complete la misma.

Una vez recibida la notificación, la AEPD inscribirá el fichero si la notificación se ajusta a lo dispuesto en la Ley y, en caso contrario, podrá pedir que se completen o se subsanen los datos notificados. Transcurrido un mes desde la presentación de la solicitud de inscripción del fichero sin que la Agencia Española de Protección de Datos haya resuelto nada, se entenderá inscrito el fichero a todos los efectos legales.

3.3 Responsable del Fichero.

La LOPD, en su artículo 3, apartado d), define al Responsable del Fichero o tratamiento de la siguiente forma: *“Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”*.

El responsable de cada fichero de la UPV será el que se haya establecido en la declaración de cada fichero ante la AEPD.

La Universidad Politécnica de Valencia define la figura del **Responsable Propietario del Fichero** como aquella persona física que efectivamente decide sobre el uso de los datos contenidos en el fichero y es responsable del uso diario de los datos contenidos en el mismo.

Los jefes de servicio o unidad que, para el cumplimiento de sus tareas administrativas, necesiten tratar datos de carácter personal, serán Responsables Propietarios de los Ficheros en el ámbito de su función y deberán velar para que el tratamiento se ajuste en todo momento a lo previsto en la ley así como asegurarse del establecimiento y cumplimiento de las disposiciones de seguridad adecuadas.

3.4. Tipo de los datos.

La LOPD identifica tres niveles de medidas de seguridad, según los datos protegidos sean de nivel BÁSICO, MEDIO o ALTO.

1. **BÁSICO:** Cuando los datos recogidos son sobre el nombre, apellidos, direcciones de contacto, teléfono y otros.
2. **MEDIO:** Cuando los datos recogidos son relativos a la comisión de infracciones penales o administrativas, información de Hacienda Pública o información de servicios financieros.
3. **ALTO:** Cuando los datos recogidos son relativos a la ideología, religión, creencias, origen racial, salud o vida.

Cuanto mayor sea el nivel de los datos, mayor número de medidas técnicas y organizativas serán necesarias para mantener la seguridad, integridad y confidencialidad de los datos.

Es conveniente por lo tanto intentar recoger los datos estrictamente necesarios para llevar a cabo las tareas requeridas, intentando evitar recoger datos que aumenten el nivel de los datos y con ello la complejidad en la recogida, almacenamiento y tratamiento de los datos. **Es especialmente importante evitar en lo posible la recogida de datos especialmente protegidos (nivel ALTO).**

3.5. Finalidad y usos del fichero.

Al efectuar la declaración del fichero ante la AEPD se debe informar de la finalidad para la que se recogen los datos contenidos en el fichero. Es importante reflexionar sobre los usos que se les va a dar a los datos recogidos para así poder establecer claramente la finalidad del fichero. Si posteriormente surgiera la necesidad de utilizar los datos para finalidades distintas de las declaradas, no podría hacerse uso de ellos, en tanto en cuanto no se modificara la declaración del fichero ante la AEPD y ésta aceptara la modificación.

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para la que los datos se hubieran recogido. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos. A estos efectos la AEPD interpreta incompatible como distinto.

Cuando se recaben los datos personales de los interesados, se debe informar al mismo de la finalidad que se declaró para el fichero que recoge los datos.

3.6. Cesiones de datos.

La cesión de datos es la comunicación de los datos de carácter personal a terceras personas distintas del Responsable del Fichero.

En el apartado 4.5 del presente documento se da una descripción detallada de las garantías que deben tener las cesiones de datos que se efectúen y la forma en que deben ser realizadas.

4. Legalización de los ficheros.

- 4.1 Información previa al interesado.
 - 4.2 Consentimiento del interesado.
 - 4.3 Calidad de los datos.
 - 4.4 Deber de secreto.
 - 4.5 Comunicación de datos personales. Cesiones.
 - 4.6 Prestaciones de servicios.
 - 4.7 Derechos de los afectados.
 - 4.7.1 Procedimiento ante peticiones de acceso, rectificación, cancelación y oposición a los datos personales.
 - 4.7.2 Derecho de acceso.
 - 4.7.3 Derecho de rectificación.
 - 4.7.4 Derecho de cancelación.
 - 4.7.5 Derecho de oposición.
-

La LOPD establece una serie de principios a los que debe ajustarse la recogida y el tratamiento de datos de carácter personal. Esos principios son los siguientes:

- a) Información al interesado.
- b) Consentimiento del interesado.
- c) Calidad de los datos.
- d) Deber de secreto.
- e) Seguridad de los datos.

4.1. Información previa al interesado.

Uno de los principios fundamentales de la LOPD es informar al interesado en el momento de la recogida de los datos, es decir, explicarle al usuario para qué se necesitan esos datos y lo que se va a hacer con ellos. De esta forma, siempre que se soliciten datos a los usuarios se debe informar claramente de:

- a) La existencia del fichero.
- b) La finalidad de la recogida de los datos.
- c) De los posibles destinatarios de los datos.
- d) De si es obligatorio o no introducirlos y de las consecuencias de la negativa de un usuario a la hora de introducir determinados datos.

- e) De cómo ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- f) De la identidad y dirección del responsable del fichero.

No será necesario suministrar la información a que se refiere el punto d) cuando dicha información resulte claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

El siguiente texto puede servir como ejemplo de la información mínima que se deberá ofrecer al interesado en el momento de la recogida de los datos:

“De acuerdo con la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal y STC 292/2000, le informamos de que sus datos serán incorporados en un fichero automatizado con una finalidad exclusivamente administrativa. El interesado podrá dirigirse a la UPV, como responsable de los ficheros, para ejercer su derecho de acceso, rectificación, cancelación y oposición. El fichero se encuentra en el sistema informático de la UPV en el Camino de Vera s/n.”

4.2. Consentimiento del interesado.

Para incluir datos de carácter personal en un fichero es necesario el consentimiento de la persona de la que se recaban los datos. Este consentimiento debe ser específico para el tratamiento de datos e informado, que implica que previamente a la recogida de datos debe suministrarse al afectado la información a la que nos referimos en el apartado anterior de este manual.

Por excepción, no será necesario consentimiento del afectado cuando los datos los recoja la Administración Pública en ejercicio de sus funciones, cuando se refieran a las partes en un contrato comercial, laboral o administrativo, cuando se trate de proteger un interés vital del interesado o cuando los datos se encuentren en fuentes accesibles al público y haya un interés legítimo del responsable del fichero o del destinatario de los datos.

La UPV recogerá los datos personales necesarios en virtud de la relación que exista con el interesado; con el consentimiento, expreso o tácito, de los afectados, cuando su recogida no se desprenda de la propia relación.

4.3. Calidad de los datos.

Uno de los principios fundamentales de la LOPD que hay que respetar es el de calidad de los datos. El artículo 4 de la LOPD se ocupa en líneas generales de las condiciones en que han de realizarse las operaciones con datos personales (recogida, tratamiento y posibles comunicaciones y cesiones de los mismos):

La calidad de los datos se concreta en:

- Los datos recogidos deben ser **adecuados, pertinentes y no excesivos** en relación con el ámbito y las finalidades que han de ser determinadas, explícitas y legítimas.

- Los datos **no se podrán usar para finalidades distintas** a la finalidad para la cual fueron recogidos.
- Los datos deben ser **exactos y puestos al día** de forma que respondan a una situación actual. En el caso de que los datos sean inexactos, deberán ser rectificadas o cancelados, reconociendo en todo caso la posibilidad de acceso por parte del interesado.
- Los datos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recogidos.
- Queda prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos.

La UPV en cumplimiento de la LOPD, recogerá, procesará, almacenará, y utilizará, sólo los datos personales necesarios relacionados con su tipo de actividad y para llevar a cabo las relaciones con alumnos, proveedores, y otras personas físicas. Los datos se recogerán en virtud de la relación que exista; con el consentimiento, expreso o tácito, de los afectados, cuando su recogida no se desprenda de la propia relación.

4.4. Deber de secreto.

Tanto el responsable del fichero como toda aquella persona que intervenga en el tratamiento del mismo están obligados a mantener el secreto profesional respecto de los datos incluidos en el fichero, lo que implica la prohibición de revelar a terceras personas tales datos. Este secreto se deberá mantener incluso una vez finalizada la relación laboral.

4.5. Comunicación de datos personales. Cesiones.

Por cesión o comunicación de datos se entiende toda revelación de datos de carácter personal realizada a una persona, física o jurídica, distinta del interesado.

Como norma general, los datos de carácter personal incorporados a un fichero de datos **no pueden comunicarse** a terceras personas.

En todo caso, si es necesario realizar la cesión o comunicación de datos, **se requiere el consentimiento** del afectado. No obstante, **no se precisaría consentimiento** cuando la comunicación de los datos se produce entre las unidades de un Organismo o Ente Público, que previamente los habría recabado para el ejercicio de sus funciones, cuando la cesión sea a otras Administraciones Públicas para el ejercicio de competencias que no sean diferentes o versen sobre materias distintas y en los demás casos que establece la LOPD en su art. 11.2.

En definitiva, **no será necesario el consentimiento** del interesado para la comunicación de los datos en los siguientes supuestos citados por la LOPD:

- Cuando la cesión esté autorizada en una ley.
- Cuando se trate de datos recogidos en fuentes accesibles al público.
- **Cuando la cesión derive de una relación jurídica legítima y libremente aceptada cuyo desarrollo, cumplimiento y control haga necesaria la comunicación y siempre que ésta se limite a la finalidad que la justifica.**
- Cuando tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, Tribunales, Tribunal de Cuentas u órganos semejantes de las Comunidades Autónomas.
- **Cuando la comunicación se produzca entre las Administraciones Públicas para el posterior tratamiento de los datos con fines históricos, estadísticos o científicos.**
- Cuando se trate de datos relativos a la salud y la comunicación sea necesaria para solucionar una urgencia o para realizar estudios epidemiológicos.

La cesión de datos especialmente protegidos que revelen la ideología, religión, creencias, salud, origen racial o vida sexual sólo podrán ser comunicados con el consentimiento expreso del afectado.

El consentimiento del interesado para la comunicación de los datos es **revocable** y será nulo si el interesado no ha sido informado de la finalidad a que se destinarán los datos que van a ser comunicados o del tipo de actividad de la persona a la que se comunicarán.

Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Como **excepción**, la comunicación de los datos es posible cuando se aplique a los datos un procedimiento de **disociación**, que implica que la información que se desprende de los datos no puede asociarse a una persona determinada o determinable.

En ningún caso se considerará comunicación de datos el acceso de un tercero a éstos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

4.5.1. Procedimiento ante peticiones de cesión o comunicación de datos.

Con la finalidad de que pueda analizarse la procedencia o no de una cesión o comunicación de datos, las solicitudes deberán dirigirse al Responsable Propietario del Fichero, quién podrá solicitar informe al Servicio Jurídico de esta Universidad para decidir si procede o no realizar la cesión de los datos.

Si la petición de cesión de datos se resuelve favorablemente, el Responsable del Propietario del Fichero comunicará al peticionario la decisión adoptada y procederá a realizar la transferencia de los datos requeridos previo registro de la cesión. Se recordará expresamente al peticionario que los datos cedidos sólo podrán ser utilizados para las finalidades para las que se hubieran solicitado y, además, el cumplimiento de la legislación sobre protección de datos.

En los casos de peticiones de cesión de datos resueltas desfavorablemente, el Responsable Propietario del Fichero dirigirá escrito a los peticionarios comunicando la resolución adoptada.

4.6. Prestaciones de servicios.

En aquellos casos en que sea necesario el acceso a los datos de carácter personal por parte de terceras personas distintas del Responsable del Fichero o del Encargado del Tratamiento, como consecuencia de la prestación de un servicio profesional o empresarial que realice dicho tercero a favor del Responsable del Fichero, es necesario que ambas partes (Responsable del Fichero y Tercero) **celebren un contrato** autorizando dicho acceso así como las condiciones del mismo. El contrato deberá constar por escrito o por cualquier medio que permita acreditar su celebración y contenido. En el **ANEXO 4** se presenta un modelo de contrato para prestaciones de servicios.

El contrato deberá contener al menos las siguientes **disposiciones**:

- Que el tratamiento de los datos por parte del tercero autorizado se hará siempre conforme a las instrucciones que indique el Responsable del Tratamiento.
- Que no se utilizarán los datos por el tercero para fines distintos de los que figuren en el propio contrato.
- Que los datos no se comunicarán por el tercero autorizado a ninguna otra persona, ni siquiera para su conservación.
- Que el tercero autorizado debe establecer las medidas de seguridad de los datos que establece la Ley de Protección de Datos de Carácter Personal.

Una vez cumplida la finalidad establecida en el contrato, el tercero autorizado deberá devolver los datos y cualquier soporte o documento en que consten tales datos.

4.7. Derechos de los afectados.

La Ley de Protección de Datos de Carácter Personal reconoce al afectado o interesado una serie de derechos en relación con sus datos de carácter personal.

Los interesados tendrán derecho al acceso, rectificación, cancelación y oposición de sus datos de carácter personal sometidos a tratamiento automatizado. Estos derechos tienen **carácter personal**, por lo cual solo pueden ser ejercidos por el titular de los datos. Podrá, no obstante, actuar su representante legal cuando el titular sea menor de edad o esté declarado incapaz para el ejercicio de sus derechos.

Para hacer uso de estos derechos, el titular o su representante legal deberán estar **identificados mediante su DNI** y aportar fotocopia compulsada del mismo, así como la documentación correspondiente para justificar los cambios, cancelación u oposición.

Si los datos de carácter personal resultan ser inexactos o incompletos, inadecuados o excesivos, el afectado podrá pedir del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos. También podría solicitarse la cancelación de los datos cuando se trate de revocación del consentimiento previamente otorgado, si ésta resulta procedente.

Las solicitudes de rectificación deberán indicar el dato que es erróneo y la corrección a realizar, debiéndose acompañar la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del afectado.

La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

El personal de la Universidad Politécnica de Valencia que preste servicio en las distintas unidades administrativas de la UPV y esté designado para llevar a cabo estas funciones, deberá tener un adecuado y completo conocimiento de los plazos y procedimientos legalmente establecidos para la gestión de dichos derechos.

No se exigirá contraprestación alguna por el ejercicio de los derechos.

4.7.1. Procedimiento ante peticiones de acceso, rectificación, cancelación y oposición a los datos personales.

Los distintos centros, departamentos, áreas, institutos, servicios y unidades de la Universidad Politécnica de Valencia son los encargados de atender, gestionar y tramitar los derechos de los interesados, conforme a los procedimientos que se establecen en el presente manual.

Posteriormente a la **recepción en el registro de entrada** de la solicitud del interesado según el modelo establecido al efecto (**ANEXO 5**), y la posterior remisión al órgano a que vaya dirigido, los responsables propietarios de los ficheros afectados, una vez comprobada la pertinencia de la solicitud, deben adoptar las medidas conducentes a satisfacer la petición y deben notificar los resultados a la persona interesada en los plazos preceptivos.

Si se registra de entrada una petición que no está dirigida a ninguno de los servicios o unidades que figuran como órganos frente a los cuales ejercer los derechos, ésta será tramitada a Secretaría General, que informará de la circunstancia al jefe del servicio o unidad responsable interno de los datos, para que actúe como en el caso anterior.

Las solicitudes acceso, rectificación, cancelación y oposición, resueltas desfavorablemente, serán notificadas igualmente a los interesados.

4.7.2. Derecho de acceso.

El interesado tiene derecho a obtener gratuitamente información sobre sus datos de carácter personal que aparecen incorporados a un fichero de datos para su tratamiento. La información comprenderá los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Tal información puede suministrarse al interesado mediante su visualización en la pantalla del ordenador o por escrito de cualquier tipo que sea perfectamente legible o inteligible y que no utilice claves o códigos que requieran el uso de dispositivos mecánicos para su lectura o comprensión.

El derecho de acceso puede ejercitarse cada doce meses, a menos que el interesado acredite un interés legítimo, en cuyo caso podrá ejercitarlo antes de transcurrir dicho plazo.

La Universidad Politécnica de Valencia deberá contestar la solicitud con independencia de que figuren o no datos personales del interesado en los ficheros.

La contestación se remitirá mediante correo certificado en el **plazo máximo de un mes** a contar desde la recepción de la solicitud. Transcurrido ese plazo sin que de forma expresa se responda a la petición del acceso, ésta podrá entenderse desestimada a efectos de la interposición de reclamación a la AEPD por parte del interesado.

Denegación del acceso.

Únicamente se denegará el acceso a los datos de carácter personal cuando:

- a) La solicitud sea formulada por persona distinta del afectado.
- b) El derecho se haya ejercitado en un intervalo inferior a 12 meses y no se acredite un interés legítimo al efecto.



Modelo de solicitud de acceso a los datos personales de los ficheros de la UPV.



UNIVERSIDAD
POLITECNICA
DE VALENCIA

**Solicitud de acceso a los
datos personales de los ficheros de la
UNIVERSIDAD POLITÉCNICA DE VALENCIA**

DATOS DEL SOLICITANTE:

D./D ^a :	
Domicilio:	Cod.Postal:
Localidad:	Provincia:
Dirección de email:	Teléfono:
Vinculación con la UPV:	<input type="checkbox"/> PDI - Depto:
	<input type="checkbox"/> PAS
	<input type="checkbox"/> Alumno - Centro:
	<input type="checkbox"/> Otros: (especificar)

De acuerdo con el artículo 15 de la Ley orgánica 15/1999, de protección de datos de carácter personal, y los artículos 12 y 13 del Real decreto 1332/1994, de 20 de Junio, que la desarrolla,

SOLICITO:

1. Que se me facilite gratuitamente el acceso al fichero _____ de la Universidad Politécnica de Valencia donde consten mis datos personales en el plazo máximo de un mes a contar desde la recepción de esta solicitud¹.
2. Que si la solicitud del derecho de acceso fuese estimada, se remita por correo certificado la información a la dirección arriba.
3. Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los usos concretos y de las finalidades para las cuales se guardan.

(Firma)

....., de de 2.....

Documentación que se debe adjuntar: Fotocopia compulsada del DNI.

¹ Si en el plazo de un mes no se obtiene respuesta debe considerarse denegada la petición y se podrá interponer una reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos, en virtud de los artículos 18 de la Ley orgánica 15/1999 y 17 del Real decreto 1332/1994.

Destino: _____
(unidad responsable del fichero)

4.7.3. Derecho de rectificación.

Serán rectificadas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la LOPD, en particular cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos.

La contestación se remitirá mediante correo certificado en el **plazo máximo de diez días** a contar desde la recepción de la solicitud. Transcurrido ese plazo sin que de forma expresa se responda a la petición de rectificación, ésta podrá entenderse desestimada a efectos de la interposición de reclamación a la AEPD por parte del interesado.

Cesiones previas

Si los datos rectificadas hubieran sido cedidos previamente, la Universidad Politécnica de Valencia deberá notificar la rectificación efectuada al cesionario, en el plazo de diez días, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la rectificación.

Denegación de la rectificación.

Únicamente se denegará la rectificación de los datos de carácter personal cuando se trate de datos que reflejen hechos contrastados en un procedimiento administrativo, siempre que coincidan con éste.



Modelo de solicitud de rectificación de los datos personales de los ficheros de la UPV. (anverso)



UNIVERSIDAD
POLITECNICA
DE VALENCIA

**Solicitud de rectificación de los
datos personales de los ficheros de la
UNIVERSIDAD POLITÉCNICA DE VALENCIA**

DATOS DEL SOLICITANTE:

D./D ^a :	
Domicilio:	Cod.Postal:
Localidad:	Provincia:
Dirección de email:	Teléfono:
Vinculación con la UPV:	<input type="checkbox"/> PDI - Depto:
	<input type="checkbox"/> PAS
	<input type="checkbox"/> Alumno - Centro:
	<input type="checkbox"/> Otros: (especificar)

De acuerdo con el artículo 16 de la Ley orgánica 15/1999, de protección de datos de carácter personal, y los artículos 15 y 16 del Real decreto 1332/1994, de 20 de Junio, que la desarrolla,

SOLICITO:

1. Que se proceda gratuitamente a la efectiva corrección en el plazo máximo de diez días a contar desde la recepción de esta solicitud, de los datos inexactos relativos a mi persona que se encuentren en el fichero
2. Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.
3. Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.
4. Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

(Firma)

..... de de 2.....

Documentación justificativa adjunta:

1.
2.
3.
4.
5.

Documentación que se debe adjuntar: Fotocopia compulsada del DNI.

Destino:
(unidad responsable del fichero)



Modelo de solicitud de rectificación de los datos personales de los ficheros de la UPV. (reverso)



UNIVERSIDAD
POLITECNICA
DE VALENCIA

**Solicitud de rectificación de los
datos personales de los ficheros de la
UNIVERSIDAD POLITÉCNICA DE VALENCIA**

ANEXO

Datos de que se deben rectificar:

1. Donde dice:
Debe decir:
2. Donde dice:
Debe decir:
3. Donde dice:
Debe decir:
4. Donde dice:
Debe decir:
5. Donde dice:
Debe decir:
6. Donde dice:
Debe decir:
7. Donde dice:
Debe decir:
8. Donde dice:
Debe decir:
9. Donde dice:
Debe decir:
10. Donde dice:
Debe decir:

(Firma)

....., de de 20.....

4.7.4. Derecho de cancelación.

Serán cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la LOPD, en particular cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos.

La Universidad Politécnica de Valencia deberá contestar a la solicitud que se le dirija, comunicando la cancelación o su denegación motivada.

La contestación se remitirá mediante correo certificado en el **plazo máximo de diez días** a contar desde la recepción de la solicitud. Transcurrido ese plazo sin que de forma expresa se responda a la petición de rectificación, ésta podrá entenderse desestimada a efectos de la interposición de reclamación a la AEPD por parte del interesado.

Cesiones previas.

Si los datos cancelados hubieran sido cedidos previamente, la Universidad Politécnica de Valencia deberá notificar la cancelación efectuada al cesionario, en el plazo de diez días, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

Denegación de la cancelación.


Si existe una normativa que impide que se puedan cancelar los datos o que permite u obliga a conservarlos, puede denegarse la cancelación de los mismos, haciéndoselo saber al reclamante.

Bloqueo de los datos.

La cancelación de los datos produce su bloqueo, quedando los datos a disposición de la Administración Pública y de los Tribunales para determinar las responsabilidades que procedan. Una vez prescrita la responsabilidad, se suprimirán los datos.

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 Universidad Politécnica de Valencia y el interesado (art. 16 LOPD).

Modelo de solicitud de cancelación de los datos personales de los ficheros de la UPV.



UNIVERSIDAD
POLITECNICA
DE VALENCIA

**Solicitud de cancelación de los
datos personales de los ficheros de la
UNIVERSIDAD POLITÉCNICA DE VALENCIA**

DATOS DEL SOLICITANTE:

D./D ^a :		Cod.Postal:	
Domicilio:		Provincia:	
Localidad:		Teléfono:	
Dirección de email:			
Vinculación con la UPV:	<input type="checkbox"/> PDI - Depto:		
	<input type="checkbox"/> PAS		
	<input type="checkbox"/> Alumno - Centro:		
	<input type="checkbox"/> Otros: (especificar)		

De acuerdo con el artículo 16 de la Ley orgánica 15/1999, de protección de datos de carácter personal, y los artículos 15 y 16 del Real decreto 1332/1994, de 20 de Junio, que la desarrolla,

SOLICITO:

1. Que en el plazo de diez días desde la recepción de esta solicitud, se proceda a la efectiva cancelación de todos los datos relativos a mi persona que se encuentren en el fichero _____, en los términos previstos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y me lo comuniquen de forma escrita a la dirección arriba indicada.
2. Que, en el caso de que el responsable del fichero considere que la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

(Firma)

..... de de 2.....

Documentación que se debe adjuntar: Fotocopia compulsada del DNI.

Destino: _____
(unidad responsable del fichero)

4.7.5. Derecho de oposición.

En aquellos casos en que no es necesario el consentimiento del interesado para el tratamiento de sus datos de carácter personal, dicho interesado podrá oponerse al tratamiento de sus datos dirigiéndose al Responsable del Fichero, siempre que una ley no disponga lo contrario y su oposición se base en motivos fundados y legítimos relativos a una concreta situación personal.

El Derecho de Oposición ha sido incorporado por la LOPD como consecuencia de la transposición de la Directiva 95/46, por lo que su regulación aún no ha sido objeto de desarrollo.

El interesado podrá oponerse al tratamiento de los datos que le conciernen cuando:

- a) Los datos son obtenidos de fuentes accesibles al público o de terceras personas distintas del interesado y no es necesario su consentimiento.
- b) Una ley no disponga lo contrario.
- c) Existan motivos fundados y legítimos relativos a una concreta situación personal.



Modelo de solicitud de oposición al tratamiento de los datos personales de los ficheros de la UPV.



UNIVERSIDAD
POLITECNICA
DE VALENCIA

**Solicitud de oposición al tratamiento de los
datos personales de los ficheros de la
UNIVERSIDAD POLITÉCNICA DE VALENCIA**

DATOS DEL SOLICITANTE:

D./D ^a :	
Domicilio:	Cod.Postal:
Localidad:	Provincia:
Dirección de email:	Teléfono:
Vinculación con la UPV:	<input type="checkbox"/> PDI - Depto:
	<input type="checkbox"/> PAS
	<input type="checkbox"/> Alumno - Centro:
	<input type="checkbox"/> Otros: (especificar)

De acuerdo con los artículos 6.4 y 17 de la Ley orgánica 15/1999, de protección de datos de carácter personal,

SOLICITO:

1. Que los datos referentes a mi persona que se encuentren en los ficheros de la Universidad Politécnica de Valencia sean excluidos de cualquier tratamiento, y me lo comuniquen de forma escrita a la dirección arriba indicada.
2. Que, en el caso de que el responsable del fichero considere que la oposición al tratamiento no procede, lo comunique igualmente, de forma motivada, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

Motivos por los que se opone al tratamiento de los datos:

.....

.....

.....

.....

.....

(Firma)

..... de de 2.....

Documentación que se debe adjuntar: Fotocopia compulsada del DNI.

Destino: _____

5. Notificación, Gestión y Respuesta ante Incidencias.

- 5.1. Notificación, gestión y respuesta ante Incidencias.
 - 5.2. Procedimiento de Registro de Incidencias.
 - 5.3. Procedimiento de Notificación de Incidencias.
 - 5.4. Modelo de Comunicación de Incidencias.
-

5.1. Notificación, gestión y respuesta ante Incidencias.

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad de los ficheros, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de las incidencias que comprometan la seguridad de un fichero es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para la persecución de los responsables de los mismos.

Los problemas que surjan relacionados con las medidas de seguridad de los datos de carácter personal, deberán quedar anotados en el registro de incidencias.

Para aquellos ficheros a los que el ASIC de soporte, el ASIC habilitará un **Registro de Incidencias** a disposición de todos los usuarios y administradores del fichero con el fin de que se registre en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación por escrito al responsable de seguridad o al gestor de incidencias para su registro y gestión. El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del fichero por parte de ese usuario.

5.2. Procedimiento de Registro de Incidencias.

Se habilitará un registro en el que se recoja información de las incidencias que pudieran afectar a la seguridad de los datos de carácter personal recogidos en los ficheros, y que tendrá orden cronológico.

Los campos previstos por cada incidencia serán los siguientes, tratando de cubrir todos, aunque sea posteriormente:

- Fecha y hora en que se notifica la incidencia.
- Fecha y hora en que se produjo si es descrita.
- Descripción del tipo de incidencia: acceso indebido, pérdida de datos, copia no autorizada, corrupción de datos... y explicación así como recursos afectados.
Posible inclusión o referencia de documentos, memoranda, registros de ordenador (“log”), manuales técnicos, comunicaciones del personal de seguridad del edificio, en definitiva, cualquier información que pueda resultar válida.
- Persona que ha realizado la notificación de la incidencia.
- Persona a la que se ha comunicado.
- Persona que ha incorporado la incidencia al registro.
- Posibles causas de la incidencia si se conocen.
- Efectos derivados de la incidencia.
- Medidas adoptadas y controles implantados o reforzados.
- Fecha de “cierre” de la incidencia.
- Persona que ha cerrado la incidencia.

(Los campos señalados con ▪ se exigen en el Reglamento)

5.3. Procedimiento de Notificación de Incidencias.

Cualquier persona que conozca hechos o circunstancias que puedan constituir una incidencia, especialmente si implica un riesgo respecto a la seguridad de los datos automatizados de carácter personal, los pondrá en conocimiento, preferentemente, por escrito (considerándose válido el correo electrónico como medio) del responsable propietario del Fichero y/o del responsable de seguridad de la información, quienes recabarán la información complementaria necesaria en cada caso.

La comunicación se hará utilizando el *modelo de comunicación de incidencias* que se presenta más adelante en este documento.

5.4. Modelo de Comunicación de Incidencias.

FORMULARIO DE COMUNICACIÓN DE INCIDENCIAS DE SEGURIDAD LOPD		UNIVERSIDAD POLITECNICA DE VALENCIA		ÁREA DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES
	FORMULARIO DE COMUNICACIÓN DE INCIDENCIAS DE SEGURIDAD LOPD			
	INCIDENCIA Nº :	<input type="text"/>	(A ser rellenado por el Gestor de Incidencias)	
	Fichero objeto de la Incidencia:			
	Fecha de Notificación:			
	Información sobre la Incidencia:			
	Tipo de Incidencia:	(Anotar todos los detalles de interés de la incidencia)		
	Descripción detallada de la Incidencia:			
	Fecha de la Incidencia:		Hora de la Incidencia:	
	Efectos que puede producir:	(Tanto si se ha subsanado como si no)		
Información sobre la comunicación:				
Persona(s) que realiza la comunicación:	(Especificar si son usuarios o no del Fichero)			
Persona(s) a quien(es) se comunica:				
Persona que realiza la comunicación:				
Fdo.: _____				
Área de Sistemas de Información y Comunicaciones Edificio 4L Camino de vera, s/n. 46022 VALENCIA ● Tel.(+34) 963 87 70 70 ● Fax (+34) 963 87 70 79 E-Mail: asic@cc.upv.es ● Web: http://www.upv.es/asic				

6. *Protección de los ficheros. Reglamento de Seguridad.*

- 6.3 Reglamento de Medidas de Seguridad.
 - 6.4 El Documento de Seguridad.
-

6.1. Reglamento de Medidas de Seguridad.

El artículo 9 de la LOPD, establece que el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

El desarrollo de las medidas de seguridad a implantar viene especificado en el **RD 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 (ANEXO 6)**. Este Reglamento establece tres niveles de seguridad en función de la naturaleza de los datos que se vayan a tratar: nivel básico, medio y alto. Dependiendo del nivel de los datos las medidas técnicas y organizativas a implantar serán más exigentes.

- a) **Nivel Básico:** Todos los ficheros que contengan datos de carácter personal, cualquiera que sea el tipo o la naturaleza de los datos incluidos en los mismos.
- b) **Nivel Medio:** Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

Además, 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.

- c) **Nivel Alto:** Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que determina el RD 994/1999 de 11 de junio con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

El artículo 44.3.h. de la LOPD, califica de infracción grave, el mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones.

La siguiente tabla recoge un resumen de las medidas de seguridad que se deben aplicar a los ficheros según el RD 994/1999 de 11 de junio:

Nivel BÁSICO
Redacción del <i>Documento de Seguridad</i> .
Definición de las funciones y obligaciones del personal con acceso al fichero.
Registro y notificación de incidencias.
Definición de los procedimientos de identificación y autenticación de usuarios.
Control de acceso a los recursos protegidos.
Gestión de soportes que almacenan datos del fichero.
Copias de respaldo y recuperación del fichero.

Nivel MEDIO
Todas las medidas de seguridad de nivel básico.
Designar un <i>responsable de seguridad</i> .
Auditoría bianual.
Identificación y autenticación inequívoca y personalizada, limitar intentos.
Control de acceso físico a los locales donde se encuentren los ficheros.
Gestión de soportes: registro de entrada/salida y procedimiento de desechado.
Registro y notificación de incidencias nivel medio.
Procedimientos para pruebas con datos reales.

Nivel ALTO
Todas las medidas de seguridad de los niveles básico y medio.
Cifrado en las telecomunicaciones y en la distribución de soportes.
Registro de los accesos a cada registro del fichero.
Medidas adicionales de copias de respaldo y recuperación.

6.2. El Documento de Seguridad.

Las medidas de seguridad que se adopten deben constar en el llamado *Documento de Seguridad* que debe redactar el Responsable del Fichero. Las medidas de seguridad recogidas en el este documento son de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. **Es responsabilidad del responsable del fichero adoptar 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.**

El Reglamento establece que la elaboración del Documento de Seguridad es obligatoria siempre que se traten datos de carácter personal, independientemente del nivel de seguridad al que correspondan los datos. El contenido del Documento será diferente según el nivel de seguridad que sea aplicable en cada caso atendida la naturaleza de los datos incorporados al fichero.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios en el sistema de información o en la organización del mismo.

Se considera una infracción grave "Mantener lo ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen" Artículo 43.h) LOPD.

El ASIC ha redactado el Documento de Seguridad con las medidas técnicas y organizativas a aplicar para mantener la seguridad de aquellos ficheros alojados en los servidores gestionados por el ASIC. Dicho documento está disponible para que los distintos responsables de los ficheros lo consulten y divulgen y para servir de modelo para la confección por parte de otras unidades del documento de seguridad para sus propios ficheros.

Los Responsables de Fichero serán los encargados de tomar las medidas oportunas para que cada usuario con acceso al fichero conozca aquellos contenidos del Documento de Seguridad que sean relevantes para el desarrollo de sus funciones. **Es su responsabilidad por lo tanto asegurarse de que cada usuario conoce sus obligaciones y responsabilidades en el ámbito de la gestión de datos personales y conoce igualmente los procedimientos definidos en la UPV para la gestión de los datos personales.**

ANEXOS.

- ANEXO 1. Regulación de los ficheros automatizados de datos de carácter personal de la UPV.
- ANEXO 2. Modelo normalizado para la declaración ante la AEPD de ficheros con datos de carácter personal.
- ANEXO 3. Modelo de resolución de creación, modificación o supresión de fichero a insertar en el DOGV.
- ANEXO 4. Modelo de contrato para prestaciones de servicios.
- ANEXO 5. Modelos de solicitudes para el ejercicio de los derechos de los interesados.
- ANEXO 6. Legislación aplicable e instrucciones AEPD.
- Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD).
 - R.D. 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.
 - Instrucciones AEPD.
- ANEXO 7. Preguntas más frecuentes.
- Ficheros en soporte papel o ficheros manual-estructurados.
- ANEXO 8. Comunicaciones internas sobre protección de datos personales.
-



ANEXO 1. Regulación de los ficheros automatizados de datos de carácter personal de la UPV.



ANEXO 2. Modelo normalizado para la declaración ante la AEPD de ficheros con datos de carácter personal.



ANEXO 3. Modelo de resolución de creación, modificación o supresión de fichero a insertar en el DOGV.



ANEXO 4. Modelo de contrato para prestaciones de servicio.



ANEXO 5. Modelos de solicitudes para el ejercicio de los derechos de los interesados.



ANEXO 6. Legislación aplicable.

- Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD).
- R.D. 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.
- Instrucciones AEPD.



ANEXO 7. Preguntas más frecuentes.

Ficheros en soporte papel o ficheros manual-estructurados.

(Extraído del libro “El Documento de Seguridad. Análisis técnico y jurídico . Modelo” de Emilio del Peso Navarro, Miguel Ángel Ramos González y Mar del Peso Ruiz. Ed. Díaz de Santos, 2004).

Cuando se habla de ficheros de datos personales, se piensa inicialmente en tratamiento de datos informatizados. Sin embargo, la LOPD no se extiende únicamente a ficheros informatizados sino también a tratamientos de datos personales no automatizados, es decir, en soporte papel.

La LOPD sólo abarca a los ficheros estructurados y no a las carpetas que no están estructuradas. Para que pueda hablarse de un fichero manual-estructurado, éste debe estructurarse conforme a criterios específicos relativos a las personas que faciliten el acceso fácil a los datos.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la LOPD deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 2005, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

En relación a los ficheros y tratamientos no automatizados anteriores a la LOPD, se puede afirmar que les sería de aplicación estrictamente la Disposición Adicional Primera, por lo que su adecuación a la LOPD deberá cumplirse el 24 de octubre de 2007. Las obligaciones mencionadas expresamente en esta Disposición son las referidas a la declaración del fichero. Las medidas de seguridad a implantar en estos ficheros deben ser establecidas por un reglamento de medidas de seguridad para los ficheros manuales, que debe ser aprobado por el Gobierno y que les será de aplicación a partir de esa fecha. Los derechos de acceso, rectificación y cancelación pueden ser ejercidos por los interesados sin esperar a esa fecha.

Conclusiones:

- Vigencia para los tratamientos de datos personales en soporte papel de los derechos de acceso, rectificación y cancelación.
- No es de aplicación la normativa de seguridad a los ficheros manuales, bien por inexistencia de la normativa en el caso de ficheros posteriores a la LOPD, bien por imposibilidad de aprobar ésta hasta el 2007 en el caso de ficheros preexistentes a la LOPD.
- Incertidumbre respecto de la obligación de declarar los ficheros manuales y de inscribirlos en los Registros de Protección de Datos Personales.



ANEXO 8. Comunicaciones internas sobre protección de datos personales.

