



## ÍNDICE

### I. Disposiciones Generales

- Aprobación de las Instrucciones de Servicio sobre el tratamiento de datos de carácter personal ..... 418
- Instrucciones de Servicio sobre el tratamiento de datos de carácter personal ..... 418

A. Funciones y responsabilidades del personal implicado en el tratamiento de datos .....	418
A.1 Tipos de obligaciones y responsabilidades .....	418
A.2 Personal implicado en el tratamiento de datos .....	418
A.3 Obligaciones genéricas de los usuarios .....	419
A.4 Funciones del encargado interno del tratamiento .....	420
A.5 Funciones del responsable interno del tratamiento .....	420
A.6 Funciones del Gerente .....	421
A.7 Funciones del responsable de seguridad .....	422
A.8 Funciones del encargado de aplicaciones .....	422
A.9 Funciones del encargado de sistemas .....	423
A.10 Funciones del encargado de comunicaciones .....	423
A.11 Funciones de los técnicos informáticos .....	423
A.12 Funciones del encargado de procesos .....	424
A.13 Funciones del Gabinete Jurídico .....	424
B. Régimen general de tratamiento y comunicación interna de información de carácter personal .....	425
B.1 Tratamiento y comunicación interna de la información ..	425
B.1.1 Cuadros de acceso a información de carácter personal ...	425
B.1.2 Clasificación de los datos personales .....	425
B.1.3 Clases de usuarios .....	427
B.1.4 Cuadro de acceso a la información de estudiantes .....	428
B.1.5 Cuadro de acceso a la información personal de personal docente e investigador .....	429
B.1.6 Cuadro de acceso a la información personal de personal de administración y servicios .....	429
B.2 Procedimiento de comunicación interna de datos .....	430
C. Registro de incidencias .....	431
C.1 Registro informatizado de incidencias.	
Gestión de incidencias .....	431
Anexo 1. Modelo de comunicación interna de datos de carácter personal .....	432
Anexo 2. Pantallas del registro informatizado de incidencias ..	433

## I. Disposiciones Generales

*Resolución de 30 de mayo de 2003, del Gerente de la Universidad de Zaragoza, por la que se dispone la aprobación de las Instrucciones de Servicio sobre el **tratamiento de datos** de carácter personal.*

La entrada en vigor de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (BOE de 14 de diciembre), que amplía su ámbito de aplicación a los ficheros de datos de carácter personal no automatizados, así como la experiencia acumulada en la gestión de los ficheros de datos de carácter personal, aconsejó una reestructuración de los mismos con el fin de lograr el equilibrio deseado entre los principios de protección de la privacidad del individuo y de eficacia y transparencia en la gestión de la Universidad. Así, en virtud de la resolución de la Universidad de Zaragoza de fecha 16 de julio de 2001 (BOA de 13 de agosto), se llevó a cabo la tarea de reestructuración de ficheros, mediante la supresión de los antiguos ficheros de datos de carácter personal de la Universidad de Zaragoza y la creación de los nuevos ficheros de personal, estudiantes, terceros y datos médicos de la Universidad de Zaragoza.

La reestructuración de los ficheros de la Universidad de Zaragoza fue un primer paso en el proceso global de adaptación del tratamiento de datos de la Universidad a las exigencias de la norma, a las necesidades de la gestión universitaria y a las peticiones de la sociedad. Para dar

cumplida respuesta a esas necesidades y lograr un adecuado cumplimiento de la normativa vigente en materia de protección de datos en el ámbito de la Universidad de Zaragoza, se ha adoptado la resolución de 6 de junio de 2002 en virtud de la cual se aprueba la normativa propia de la Universidad de Zaragoza en protección de datos de carácter personal, publicada en el BOA de 19 de junio.

Como complemento necesario a la regulación propia en materia de protección de datos de carácter personal, es oportuna la organización y diseño interno de las funciones y responsabilidades del personal, el régimen de tratamiento y comunicación interna de la información y la implantación de las medidas de seguridad establecidas en la normativa vigente.

Por todo ello, y en virtud de las competencias que me otorgan la citada resolución de la Universidad de Zaragoza de fecha 16 de julio de 2001 y lo indicado en los Estatutos de esta Universidad, dispongo:

Artículo único. La aprobación de las instrucciones de servicio sobre el tratamiento de datos de carácter personal que se adjuntan, que serán de obligado cumplimiento para todo el personal de la Universidad, desde el día 1 de junio de 2003.

Zaragoza, a 30 de mayo de 2003. El Gerente, Mariano Berge Andrés

### INSTRUCCIONES DE SERVICIO SOBRE EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

#### A. FUNCIONES Y RESPONSABILIDAD DEL PERSONAL IMPLICADO EN EL TRATAMIENTO DE DATOS

##### A.1 Tipos de obligaciones y responsabilidades

1. Las genéricas de todo usuario.
2. Las de supervisión y control.
3. Las relacionadas con la creación, modificación y supresión de ficheros.
4. Las relacionadas con la recogida y uso de los datos.
5. Las relacionadas con la calidad de los datos.
6. Las relacionadas con la cesión/publicidad de datos.
7. Las relacionadas con la tutela de derechos.
8. Las relacionadas con las medidas de seguridad.
9. Las relacionadas con el deber de secreto y confidencialidad.
10. Las de organización interna.

##### A.2 Personal implicado en el tratamiento de datos

- *Usuario*: toda persona que en el ejercicio de sus competencias trata datos de carácter personal.
- *Encargados internos de tratamiento*: aquellas personas de las que depende un grupo de usuarios y tienen una res-

ponsabilidad que alcanza al tratamiento de datos en una unidad concreta.

En el caso del *fichero de estudiantes* serán encargados internos de tratamiento los administradores de los centros, los administradores de los servicios universitarios, los jefes de servicio y de las unidades dependientes de la vicegerencia de asuntos académicos y el responsable de la unidad de gestión de cada estudio propio u otras figuras organizativas que puedan establecerse de acuerdo con las normas vigentes.

En el caso del *fichero de personal* serán encargados de tratamiento los administradores de los centros, los administradores de los servicios, los Directores de los departamentos y los jefes de servicio correspondientes u otras figuras organizativas que puedan establecerse de acuerdo con las normas vigentes.

En el caso del *fichero de terceros* serán encargados del tratamiento los administradores de los centros, los administradores de los servicios, los Directores de los departamentos y los jefes de servicio correspondientes u otras figuras organizativas que puedan establecerse de acuerdo con las normas vigentes.

En el caso del *fichero de datos médicos* será encargado interno del tratamiento el personal médico asignado a la Universidad de Zaragoza y las personas encargadas del servicio de ergonomía y de la tramitación de bajas y altas laborales.

Sin perjuicio de todo lo anterior el responsable interno del tratamiento de cada fichero, por necesidad o conveniencia organizativa, podrá nombrar encargados internos de tratamiento a personas que no coincidan con las figuras anteriormente señaladas.

- *Responsables internos del tratamiento*: a efectos de tratamiento de datos son los máximos responsables internos del fichero, de ellos dependen administrativamente uno o varios encargados internos de tratamiento de una o varias unidades administrativas.

El responsable interno del tratamiento del fichero de estudiantes será el Vicegerente de Asuntos Académicos.

El responsable interno del tratamiento del fichero de personal será el Vicegerente de Asuntos Administrativos.

El responsable interno del tratamiento del fichero de terceros será el Vicegerente de Asuntos Económicos.

El responsable interno del tratamiento del fichero de datos médicos será el Jefe de la Unidad de Protección y Prevención de Riesgos.

- *Responsable de seguridad*: la persona en quien el responsable del fichero delega las obligaciones que le afectan en materia de implantación, coordinación y control de las medidas de seguridad aplicables.

El responsable de seguridad de los ficheros será el Director Técnico del Servicio de Informática y Comunicaciones-Centro de Cálculo de la Universidad de Zaragoza.

- *Encargado de aplicaciones*: figura creada por el responsable de seguridad para funciones concretas.

Será encargado de aplicaciones el responsable del Área de Gestión del Servicio de Informática y Comunicaciones – Centro de Cálculo.

- *Encargado de sistemas*: figura creada por el responsable de seguridad para funciones concretas.

Será encargado de sistemas el responsable del Área de Sistemas del Servicio de Informática y Comunicaciones – Centro de Cálculo.

- *Encargado de comunicaciones*: figura creada por el responsable de seguridad para funciones concretas.

Será encargado de comunicaciones el responsable del Área de Comunicaciones del Servicio de Informática y Comunicaciones – Centro de Cálculo.

- *Técnicos Informáticos*: Personal integrado en el Centro de Cálculo que realizan funciones de diseño, administración, operación o programación de las bases de datos, aplicaciones, sistemas o equipos de comunicaciones y que por su trabajo puedan tener acceso a la información del fichero.

- *Encargado de procesos*: figura creada por el responsable del fichero, con funciones de supervisión y control. De-

pende jerárquicamente en materia de tratamiento de datos de carácter personal del responsable de seguridad.

- *Responsable del fichero*: La persona física o jurídica de naturaleza pública o privada, u órgano administrativo, que decide acerca de la finalidad, contenido y uso del tratamiento, adoptando las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal. En nuestro caso la Universidad de Zaragoza, como institución de derecho público, es la responsable de los ficheros

### A.3 Obligaciones de los usuarios: “Obligaciones genéricas”

El tratamiento de datos de carácter personal sólo podrá llevarse a cabo de acuerdo con las competencias del puesto de trabajo y de acuerdo con las finalidades de los ficheros. Todo el personal implicado en razón de sus competencias debe cumplir las siguientes obligaciones:

1. Realizar el tratamiento de datos de acuerdo con la *normativa propia* de la Universidad de Zaragoza en esta materia.
2. En el caso en que le corresponda recabar datos de carácter personal, hacerlo de acuerdo con el procedimiento establecido en la *normativa propia* de la Universidad.
3. Respetar las finalidades del fichero.
4. Informar al encargado interno del tratamiento de cualquier incidencia detectada en el tratamiento de datos.
5. Responder con la máxima celeridad a los requerimientos en materia de tratamiento de datos de los responsables internos de tratamiento, encargados internos de tratamiento y responsable de seguridad.
6. Cumplir con las medidas de seguridad adoptadas de acuerdo con lo que se especifica en el *documento de seguridad* según las indicaciones de los encargados internos del tratamiento y en su caso el personal técnico competente.
7. Respetar los procedimientos internos establecidos en la *normativa propia* sobre atención a los ejercicios de acceso, rectificación y cancelación, cesiones de datos y creación y modificación de ficheros, así como cualquier otro procedimiento interno que se establezca en materia de tratamiento de datos.
8. Respetar el régimen de tratamiento y comunicación interna de la información establecido en estas *instrucciones de servicio* en su apartado B.
9. Respetar los deberes de secreto profesional y confidencialidad de la información a la que tengan acceso aún después de dejar de ocupar su puesto de trabajo; en particular cada usuario será responsable de la confidencialidad de su contraseña personal sobre la que debe guardar reserva absoluta. Los usuarios accederán al sistema utilizando siempre el propio identificador.
10. Consultar al encargado interno del tratamiento sobre las dudas que surgiesen sobre tratamiento de datos, previa lectura de la *normativa propia* y en su caso de las *instrucciones de servicio*.

Estas obligaciones de todos los usuarios pasarán a denominarse en adelante “obligaciones genéricas”.

#### **A.4 Funciones de los encargados Internos del tratamiento**

1. Cumplimiento de las obligaciones genéricas en su calidad de usuarios.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Propuesta motivada al responsable interno del tratamiento de la necesidad de crear, modificar o suprimir ficheros.

4. Relativas a la recogida y uso de los datos:

4.1 Garantizar que los datos se recaban de forma legal y legítima para fines adecuados a las competencias de la Universidad.

4.2 Supervisar que los formularios de recogida de datos introducen las fórmulas de autorización e informativas preceptivas de acuerdo con la *normativa propia* de la Universidad.

4.3 Conservar los documentos de recogida de datos firmados por los interesados (impresos de matrícula, contratos laborales, etc).

4.4 Garantizar que el uso de los datos en su unidad es adecuado a la finalidad del fichero.

4.5 Conservar los datos durante los plazos previstos en la normativa vigente.

4.6 Promover la cancelación de oficio de los datos que no sirvan a la finalidad para la que fueron recabados y no sea preceptiva su conservación de acuerdo con la normativa vigente.

4.7 Garantizar el cumplimiento del régimen de tramitación interna de información y remitir al Gerente las solicitudes de comunicación interna en el régimen de tratamiento de la información previsto en el punto 2 del apartado B de estas *instrucciones de servicio*.

5. Relativas a la calidad de los datos:

5.1 Garantizar que los datos recabados en su unidad son adecuados, pertinentes y no excesivos en referencia a la finalidad para la que son recabados.

5.2 Actualizar los datos reflejando las rectificaciones en plazo de acuerdo con el Título II de la *normativa propia* de la Universidad, relativo al ejercicio de los derechos de acceso, rectificación y cancelación.

5.3 Cancelar los datos cuando así se resuelva a petición del interesado, por el procedimiento establecido en el Título II de la *normativa propia* de la Universidad relativo al ejercicio de los derechos de acceso, rectificación y cancelación.

6. Relativas a la cesión/publicidad de datos: Ninguna específica.

7. Relativas a la tutela de derechos del interesado:

7.1 Mantener los archivos organizados de manera que se garantice el ejercicio adecuado de los derechos del interesado.

7.2 Informar a los interesados del procedimiento de ejercicio de sus derechos (mediante escrito que adjunte documento identificativo y acreditativo), cuando éstos se interesen por ello.

7.3 Remitir al responsable interno del tratamiento (a su solicitud) en el plazo máximo de diez días (para accesos) o cinco días (rectificación y cancelación), la información relativa a los interesados que hayan solicitado el derecho de acceso, rectificación o cancelación.

7.4 Reflejar en los archivos las decisiones adoptadas por Gerencia sobre rectificación y cancelación de datos.

8. Relativas a medidas de seguridad:

8.1 Supervisión y orientación para el cumplimiento de las medidas de seguridad en la unidad, asesorado en su caso por el responsable de seguridad.

8.2 Regular el cambio periódico de contraseñas del personal dependiente. Para ello, solicitará los identificadores correspondientes al personal de su unidad, tramitará los nuevos identificadores en caso de olvido o bloqueo de la información y dará de baja a las personas que, por cualquier motivo, no deban tener acceso a la información.

8.3 Comunicar al responsable interno del tratamiento cualquier incidencia detectada.

9. Relativas al deber de secreto y confidencialidad:

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

10. Relativas a la organización interna:

10.1 Asignación de funciones específicas sobre tratamiento de datos al personal dependiente del encargado interno del tratamiento.

10.2 Proponer a los responsables internos del tratamiento las modificaciones que considere oportunas de los *documentos de seguridad* o de estas *instrucciones de servicio*.

#### **A.5 Funciones de los responsables internos del tratamiento**

1. Cumplimiento de las obligaciones genéricas en su calidad de usuarios.

2. Las de control de cumplimiento por parte de los encargados internos.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Propuesta motivada a Gerencia de la necesidad de crear, modificar o suprimir ficheros.

4. Relativas a la recogida y uso de los datos:

4.1 Proponer modificaciones en las fórmulas de autorización e informativas de los impresos de recogida de datos.

4.2 Asesorar sobre las solicitudes de comunicación interna de información no contempladas en el régimen de tratamiento de información previsto en el punto 2 del apartado B de estas *instrucciones de servicio*.

5. Relativas a la calidad de los datos: Ninguna función específica.

6. Relativas a la cesión/publicidad de datos:

6.1 Llevará a cabo las medidas oportunas destinadas a un control efectivo de las cesiones.

6.2 Reflejar las cesiones efectuadas en el *registro de incidencias* tal y como se especifica en la *normativa propia* de la Universidad.

7. Relativas a la tutela de derechos del interesado:

7.1 Gestionar el procedimiento interno de recogida de información a fin de contestar a los interesados que soliciten el ejercicio de los derechos de acceso, rectificación y cancelación.

7.2 Efectuar, asesorado, en su caso, por el Gabinete Jurídico, una propuesta de contestación a los derechos de acceso, rectificación y cancelación.

7.3 Comunicar al encargado interno del tratamiento correspondiente la rectificación o cancelación que debe efectuarse dentro del plazo establecido en la normativa propia de la Universidad (en el Título II relativo al ejercicio de los derechos de acceso, rectificación y cancelación).

8. Relativas a medidas de seguridad:

8.1 Comunicar al responsable de seguridad cualquier incidencia detectada en la aplicación de las medidas de seguridad.

8.2 Colaborar en las auditorías internas con una periodicidad máxima de cada dos años, junto con el encargado de procesos y un representante del Gabinete Jurídico si ello fuese preciso. El informe de auditoría será emitido por el encargado de procesos. La función del responsable interno del tratamiento será de apoyo a la auditoría.

9. Relativas al deber de secreto y confidencialidad:

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

10. Relativas a la organización interna:

10.1 Asignación de funciones específicas sobre tratamiento de datos al personal dependiente del responsable interno del tratamiento.

10.2 Presencia en las inspecciones de la Agencia de Protección de Datos.

10.3 Propuesta al Rector sobre la iniciación de expedientes disciplinarios.

10.4 Proponer a Gerencia las modificaciones de los *documentos de seguridad*.

## A.6 Funciones del Gerente

1. Cumplimiento de las obligaciones genéricas en su calidad de usuario.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Propuesta al Rector de creación, modificación o supresión de ficheros. La publicación e inscripción de la creación, modificación o supresión de ficheros será decisión del Rector.

4. Relativas a la recogida y uso de los datos: Ninguna específica

5. Relativas a la calidad de los datos: Ninguna específica.

6. Relativas a la cesión de datos:

6.1 Decisión sobre la pertinencia de ceder datos que requieran de consentimiento del interesado y reflejar tal circunstancia en el *registro de incidencias* tal y como se especifica en la *normativa propia* de la Universidad.

6.2 Firma de los contratos de prestación de servicios, de acuerdo con el anexo VIII de la *normativa propia*, previo asesoramiento del Gabinete Jurídico.

6.3 Supervisar la remisión de las cartas de condiciones que serán firmadas por los cesionarios.

6.4 Conservar de forma organizada las cartas de condiciones firmadas por las empresas cesionarias.

6.5 Indicar al responsable de seguridad las cesiones que finalmente no se hubiesen efectuado a fin de que éste corrija el marcado en la ficha de los interesados.

6.6 Reflejar las cesiones efectuadas en el *registro de incidencias* tal y como se especifica en la *normativa propia* de la Universidad.

7. Relativas a la tutela de derechos del interesado:

7.1 Evaluar la adecuación formal de las solicitudes de acceso, rectificación y cancelación y en su caso instar las subsanaciones oportunas.

7.2 Distribución de las solicitudes de acceso, rectificación y cancelación a los responsables internos de tratamiento correspondientes.

7.3 Contestación a los derechos de acceso, rectificación y cancelación a propuesta del responsable interno del tratamiento.

7.4 Mantener un registro documental de accesos, rectificaciones y cancelaciones y reflejarlo en el *registro de incidencias* tal y como se establece en la normativa interna.

8. Relativas a medidas de seguridad:

8.1 Aprobación de los *documentos de seguridad*, así como de sus posibles modificaciones.

8.2 Decidir sobre la modificación con carácter general del régimen de comunicaciones internas de información.

9. Relativas al deber de secreto y confidencialidad:

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

10. Relativas a la organización interna:

10.1 Nombramiento y cese de encargados internos de tratamiento, a personas que no coincidan con las expresamente señaladas en el punto 2 del apartado A de estas *instrucciones de servicio*.

10.2 Aprobación de normativa interna en materia de protección de datos

10.3 Propuesta al Rector para la iniciación de procedimientos disciplinarios.

10.4 Coordinación de los distintos responsables internos de tratamiento del fichero.

10.5 Presencia en las inspecciones de la Agencia de Protección de Datos.

El Gerente desempeñará cualesquiera otras funciones atribuidas en virtud de la resolución de la Universidad de Zaragoza de fecha 16 de julio de 2001 reguladora de los ficheros de datos de carácter personal de la Universidad y de delegación de facultades.

## A.7 Funciones del responsable de seguridad

1. Cumplimiento de las obligaciones genéricas en su calidad de usuario.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Proponer al Gerente la creación, modificación o supresión de ficheros.

4. Relativas a la recogida y uso de los datos: Ninguna específica.

5. Relativas a la calidad de los datos:

5.1 Garantizar la coherencia interna de la información en los distintos sistemas.

6. Relativas a la cesión de datos:

6.1 Supervisar y garantizar la adecuación del procedimiento efectuado en su ámbito de actuación.

7. Relativas a la tutela de derechos del interesado:

7.1 Proporcionar la información precisada por el responsable interno del tratamiento.

8. Relativas a medidas de seguridad:

8.1 Diseño e implantación de las medidas de seguridad de los ficheros automatizados o no.

8.2 Mantener un *registro de incidencias*:

8.3 Redactar las especificaciones técnicas de los *documentos de seguridad* y sus modificaciones.

8.4 Garantizar la actualización de los anexos al *documento de seguridad* relativo a hardware, software y personal con acceso autorizado.

8.5 Controlar la comunicación interna de información. Regular el cambio periódico de contraseñas del personal dependiente.

8.6 Supervisión de la aplicación de las medidas en su ámbito de actuación.

9. Relativas al deber de secreto y confidencialidad:

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

10. Relativas a la organización interna:

10.1 Asignación de funciones específicas sobre tratamiento de datos al personal dependiente.

10.2 Propuesta al Rector sobre iniciación de expedientes disciplinarios.

10.3 Presencia en las inspecciones de la Agencia de Protección de Datos.

## A.8 Funciones del encargado de aplicaciones

1. Cumplimiento de las obligaciones genéricas en su calidad de usuario.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Proporcionar la asistencia técnica necesaria para la redacción de los nuevos ficheros, en particular en lo relativo a los campos de los ficheros.

3.2 Proponer al responsable de seguridad la creación, modificación o supresión de ficheros.

4. Relativas a la recogida y uso de los datos: Ninguna específica.

5. Relativas a la calidad de los datos:

5.1 Garantizar la coherencia interna de la información en los distintos sistemas en su ámbito de actuación.

6. Relativas a la cesión de datos:

6.1 Comprobación de las autorizaciones presentadas por los interesados.

6.2 Marcado de las cesiones en la ficha del interesado con la autorización del responsable de seguridad.

7. Relativas a la tutela de derechos del interesado:

7.1 Proporcionar las medidas técnicas adecuadas para el bloqueo de datos cuando así se precise.

7.2 Proporcionar la información precisada por el responsable de seguridad.

8. Relativas a medidas de seguridad:

8.1 Garantizar el cumplimiento de las medidas de seguridad en su ámbito de actuación.

8.2 Proponer al responsable de seguridad la implantación de nuevas medidas de seguridad en su ámbito de actuación

8.3 Proponer modificaciones a los *documentos de seguridad* en su ámbito de actuación.

8.4 Actualizar las especificaciones técnicas de los *documentos de seguridad* relativas a hardware, software y personal con acceso autorizado en su ámbito de actuación.

9. Relativas al deber de secreto y confidencialidad:

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

### A.9 Funciones del encargado de sistemas

1. Cumplimiento de las obligaciones genéricas en su calidad de usuario.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Proponer al responsable de seguridad la creación, modificación o supresión de ficheros.

4. Relativas a la recogida y uso de los datos: Ninguna específica.

5. Relativas a la calidad de los datos:

5.1 Garantizar la coherencia interna de la información en los distintos sistemas en su ámbito de actuación.

6. Relativas a la cesión de datos: Ninguna específica.

7. Relativas a la tutela de derechos del interesado: Ninguna específica.

8. Relativas a medidas de seguridad:

8.1 Garantizar el cumplimiento de las medidas de seguridad en su ámbito de actuación.

8.2 Proponer al responsable de seguridad la implantación de nuevas medidas de seguridad en su ámbito de actuación.

8.3 Proponer modificaciones a los *documentos de seguridad* en su ámbito de actuación.

8.4 Actualizar las especificaciones técnicas de los *documentos de seguridad* relativas a hardware, software y personal con acceso autorizado en su ámbito de actuación.

9. Relativas al deber de secreto y confidencialidad:

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

### A.10 Funciones del encargado de comunicaciones

1. Cumplimiento de las Obligaciones Genéricas en su calidad de usuario.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Proponer al responsable de seguridad la creación, modificación o supresión de ficheros.

4. Relativas a la recogida y uso de los datos: Ninguna específica

5. Relativas a la calidad de los datos:

5.1 Garantizar la coherencia interna de la información en los distintos sistemas en su ámbito de actuación.

6. Relativas a la cesión de datos: Ninguna específica.

7. Relativas a la tutela de derechos del interesado:

7.1 Proporcionar la información precisada por el responsable de seguridad.

8. Relativas a medidas de seguridad:

8.1 Garantizar el cumplimiento de las medidas de seguridad en su ámbito de actuación.

8.2 Proponer al responsable de seguridad la implantación de nuevas medidas de seguridad en su ámbito de actuación

8.3 Proponer modificaciones a los *documentos de seguridad* en su ámbito de actuación.

8.4 Actualizar las especificaciones técnicas de los *documentos de seguridad* relativas a hardware, software y personal con acceso autorizado en su ámbito de actuación.

9. Relativas al deber de secreto y confidencialidad:

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

### A.11 Funciones de los técnicos informáticos

1. Cumplimiento de las obligaciones genéricas en su calidad de usuario.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Proponer al responsable de seguridad la creación, modificación o supresión de ficheros.

4. Relativas a la recogida y uso de los datos: Ninguna específica.

5. Relativas a la calidad de los datos: Ninguna específica.

6. Relativas a la cesión de datos: Ninguna específica.

7. Relativas a la tutela de derechos del interesado: Ninguna específica.

8. Relativas a medidas de seguridad:

8.1 Garantizar el cumplimiento de las medidas de seguridad en su ámbito de actuación.

8.2 No permitir que ninguna herramienta o programa de utilidad que permita el acceso al fichero quede accesible a ningún usuario no autorizado expresamente a ello.

8.3 Vigilar los intentos de acceso fraudulentos al fichero observando las medidas de seguridad adoptadas y proponiendo aquellas otras de carácter técnico u organizativo que mejoren la confidencialidad, integridad y disponibilidad de los datos.

8.4 Proponer al responsable de seguridad la implantación de nuevas medidas de seguridad en su ámbito de actuación.

8.5 Proponer modificaciones a los *documentos de seguridad* en su ámbito de actuación.

9. Relativas al deber de secreto y confidencialidad:

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

## A.12 Funciones del encargado de procesos

1. Cumplimiento de las obligaciones genéricas en su calidad de usuario.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros: Ninguna específica

4. Relativas a la recogida y uso de los datos:

4.1 Comprobación periódica del cumplimiento de los procedimientos internos relativos a recogida y tratamiento de datos por las distintas unidades de la Universidad de Zaragoza, de acuerdo con lo dispuesto en la *normativa propia*.

5. Relativas a la calidad de los datos: Ninguna específica.

6. Relativas a la cesión de datos:

6.1 Comprobación periódica del cumplimiento de los procedimientos internos relativos a cesiones de datos por las distintas unidades de la Universidad de Zaragoza, de acuerdo con lo dispuesto en la *normativa propia*.

7. Relativas a la tutela de derechos del interesado:

7.1 Comprobación periódica del cumplimiento de los procedimientos internos relativos a tutela de derechos por las distintas unidades de la Universidad de Zaragoza, de acuerdo con lo dispuesto en la *normativa propia*.

8. Relativas a las medidas de seguridad:

8.1 Comprobación periódica del cumplimiento de los procedimientos internos relativos a implantación y aplicación de las medidas de seguridad establecidas en el *documento de seguridad* por las distintas unidades de la Universidad de Zaragoza.

8.2 Colaboración en la elaboración de informes de seguridad y emisión de informes definitivos.

8.3 Asesoramiento en la implantación de las medidas propuestas en los *documentos de seguridad*.

9. Relativas al deber de secreto y confidencialidad.

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

## A.13 Funciones del Gabinete Jurídico

1. Cumplimiento de las obligaciones genéricas en su calidad de usuario.

2. Las de control de cumplimiento del personal dependiente.

3. Relativas a la creación, modificación o supresión de ficheros:

3.1 Redactar a propuesta de Gerencia las resoluciones sobre creación, modificación o supresión de ficheros y llevar a cabo los trámites oportunos para hacerlo efectivo (publicación y notificación a la APD para su inscripción).

4. Relativas a la recogida y uso de los datos:

4.1 Redactar a propuesta de Gerencia las fórmulas de autorización e informativas a insertar en los impresos de recogida de datos.

5. Relativas a la calidad de los datos: Ninguna específica.

6. Relativas a la cesión de datos:

6.1 Redactar a propuesta de Gerencia las “Condiciones de cesión” así como los modelos de contratos de prestación de servicios.

7. Relativas a la tutela de derechos del interesado:

7.1 Redactar las propuestas de contestación a los interesados en el ejercicio de sus derechos cuando en opinión del responsable interno del tratamiento la peculiaridad del caso lo requiera.

8. Relativas a las medidas de seguridad:

8.1 Redactar a propuesta de Gerencia la modificación de los *documentos de seguridad* de cada fichero, contando con la ayuda del responsable de seguridad para la redacción del apartado de “especificaciones técnicas”.

9. Relativas al deber de secreto y confidencialidad.

9.1 Velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación.

10. Relativas a organización interna:

10.1 Asesoramiento integral en materia de tratamiento de datos de carácter personal en todos sus aspectos.

10.2 Presencia en las inspecciones de la Agencia de Protección de Datos.

10.3 Redacción de los documentos pertinentes en el contexto de cualquier procedimiento administrativo (ante la Agencia de protección de Datos) o judicial en materia de protección de datos.

10.4 Redactar las propuestas de *normativa propia* e *instrucciones de servicio*, o instruir de otro modo oportuno al personal en materia de tratamiento de datos de carácter personal.



## B. RÉGIMEN GENERAL DE TRATAMIENTO Y COMUNICACIÓN INTERNA DE INFORMACIÓN DE CARÁCTER PERSONAL

### B.1 Tratamiento y comunicación interna de información

La gestión de todas las actividades de la universidad (docencia, investigación, servicios y actos universitarios, etc) requiere la participación de un conjunto muy amplio de personas. Para realizar una gestión rápida y eficaz es necesario, por un lado, disponer de un sistema de información corporativo que integre toda la información disponible, maximizando su rendimiento y minimizando los gastos de gestión y, por otro, que las personas implicadas en cada uno de los procesos accedan, en todo o en parte, a la información personal de los diferentes miembros de la comunidad universitaria.

Para conseguir lo expuesto con la máxima eficiencia se procede de dos maneras:

1. Definiendo un cuadro de accesos que establezca qué información personal debe estar accesible para cada universitario en función del puesto de trabajo que ocupa y, en consecuencia, de los procesos en lo que interviene. Visto desde otro punto de vista el cuadro de accesos define la forma en que debe configurarse el sistema de información corporativo de la Universidad para que de forma automática muestre a cada persona sólo la información a la que debe tener acceso.

2. No obstante lo anterior, es imposible prever toda la casuística que pueda presentarse por lo que resulta necesario establecer un procedimiento de comunicación interna de datos de carácter personal al que deberá recurrirse para las

situaciones no previstas en los cuadros de acceso o cuando los sistemas de información de la Universidad no faciliten de forma automática los datos pertinentes.

#### B.1.1 Cuadros de acceso a información de carácter personal

Para regular, con carácter general, este tratamiento procederemos de la siguiente forma:

- Clasificar la información personal de cada uno de los grandes colectivos universitarios (estudiantes, profesores y personal de administración y servicios) en 13 bloques de datos: universitarios, personales mínimos, particulares, administrativos básicos, administrativos generales, académicos, docentes básicos, docentes específicos, de investigación, económicos, de participación en actividades y servicios, de salud y sensibles y contraseñas.
- Clasificar al personal universitario en función de la necesidad que tiene de acceder a la información personal para el cumplimiento del trabajo que realiza. De esta clasificación resultan 10 clases de usuarios: todos, universidad, personal de administración y servicios (PAS), personal docente e investigador (PDI), mis profesores, gestores de información, decanos y directores de centro, directores de departamento, cargos universitarios y Rector.
- Cruzar las clasificaciones anteriores definiendo para cada clase de usuario si tiene o no permiso de acceso a cada bloque de información.

#### B.1.2 Clasificación de los datos personales

La información personal de cada uno de los colectivos universitarios se clasifica en los siguientes 13 bloques:

##### 1. DATOS UNIVERSITARIOS

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
<i>Nombre</i>	<i>Nombre</i>	<i>Nombre</i>
Centro, departamento, área y domicilio profesional (UZ)	Unidad (centro, departamento, área, ...) y domicilio profesional	Centro de estudios
Teléfono profesional (UZ)	Teléfono profesional (UZ)	
Fax profesional (UZ)	Fax profesional (UZ)	
Correo electrónico de uso profesional (UZ)	Correo electrónico de uso profesional (UZ)	Correo electrónico de uso profesional (UZ)
Categoría profesional	Categoría profesional	Titulación y curso (o equivalente) en el que estudia

##### 2. DATOS PERSONALES MÍNIMOS

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
<i>DNI</i>	<i>DNI</i>	<i>DNI</i>
Fecha de nacimiento	Fecha de nacimiento	Fecha de nacimiento

## 3. DATOS PARTICULARES

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
<i>NIP</i>	<i>NIP</i>	<i>NIP</i>
Domicilio particular	Domicilio particular	Domicilio particular: residencia permanente y temporal durante el curso
Teléfono particular	Teléfono particular	Teléfono particular: residencia permanente y temporal durante el curso
Titulación	Titulación	

## 4. DATOS ADMINISTRATIVOS BÁSICOS

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Relación jurídica Cuerpo/Escala/especialidad; grupo/categoría Contrato/nombramiento (fechas de inicio/fin; modalidad) Dedicación Situación Administrativa (fechas) Cargos (académicos, vinculados) Pertenencia a órganos de representación Puesto de trabajo (forma de acceso, fechas de acceso/fin, % desempeño) Tipo de jornada (reducciones, licencias)	Relación jurídica Cuerpo/Escala/especialidad; grupo/categoría Contrato/nombramiento (fechas de inicio/fin; modalidad) Dedicación Situación administrativa (fechas) Cargos (académicos, vinculados) Pertenencia a órganos de representación Puesto de trabajo (forma de acceso, fechas de acceso/fin, % desempeño) Tipo de jornada (reducciones, licencias)	No procede

## 5. DATOS ADMINISTRATIVOS GENERALES

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Datos completos sobre su situación administrativa	Datos completos sobre su situación administrativa	No procede

## 6. DATOS ACADÉMICOS

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Expediente académico	Expediente académico	Expediente académico

## 7. DATOS DOCENTES BÁSICOS

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Cuerpo Dedicación docente Asignaturas, horarios, etc. Horas teóricas y prácticas Total docencia de cada asignatura Número de grupos docentes	No procede	No procede

## 8. DATOS DOCENTES GENERALES

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Situación administrativa Reducciones Horas docentes disponibles	No procede	No procede

## 9. DATOS DE INVESTIGACIÓN

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Datos relacionados con la investigación desarrollada y los proyectos en que participa	Datos relacionados con los proyectos en que participa	Información sobre la investigación desarrollada y los proyectos en que participa.

## 10. DATOS ECONÓMICOS

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Datos necesarios para la realización de la nómina	Datos necesarios para la realización de la nómina	Cuentas corrientes para pago de matrícula u otros. Reducciones Becas

## 11. DATOS DE PARTICIPACIÓN EN ACTIVIDADES O UTILIZACIÓN DE SERVICIOS

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Datos recogidos en los diferentes servicios universitarios sobre la participación en sus actividades o la utilización de los servicios ofrecidos. Por ejemplo Actividades deportivas en las que se ha inscrito, Registros de utilización del correo electrónico, Otros de similares características		

## 12. DATOS DE SALUD

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Datos relativos a la salud	Datos relativos a la salud	Minusvalías

## 13. DATOS SENSIBLES Y CONTRASEÑAS

<i>PDI</i>	<i>PAS</i>	<i>Estudiantes</i>
Datos pertenecientes a los grupos anteriores pero de carácter privado solo necesarios para algún proceso concreto, p.e. la nómina	Datos pertenecientes a los grupos anteriores pero de carácter privado solo necesarios para algún proceso concreto, p.e. la nómina	Datos pertenecientes a los grupos anteriores pero de carácter privado solo necesarios para algún proceso concreto, p.e. las becas.

**B.1.3 Clases de usuarios**

A continuación se definen un conjunto de grupos homogéneos de usuarios que denominaremos clases de usuarios. En el apartado siguiente relacionaremos cada tipo de información del fichero con las diferentes clases de usuarios; un universitario concreto puede pertenecer, en función del puesto de trabajo que ocupe o el cargo que desempeñe, a una o varias clases e, incluso, tener permiso de acceso a una información en función de su pertenencia a una clase y no tenerlo en la otra.

CLASE	DESCRIPCIÓN
Todos	Todo el mundo
Universidad	Todos los universitarios: PDI, PAS, estudiantes y otras personas con vinculación con la Universidad e inscritas en su "registro" correspondiente (p.e. becarios)
PAS	Todo el personal de administración y servicios
PDI	Todos los profesores y asimilados (p.e. personal del CSIC)
Mis profesores	Los profesores de un estudiante
Gestores de la información	Se refiere a todo el personal de la unidad concreta que participa en la gestión de cada módulo de información. Por ejemplo: Expediente de un estudiante: secretaria de su centro y Servicio de Estudiantes, Unidad Sigma. Nomina: Servicio de Personal Cada módulo de información debe tener definidos quienes son las Unidades gestoras de dicha información y quién es el responsable.
Decanos y Directores de Centro	Respecto de los datos de su propio centro.
Directores de Departamento	Respecto de los datos de su propio departamento.
Cargos Universitarios	Miembros del Consejo de Dirección y Delegados especiales del Rector con responsabilidad sobre los datos de los que se trate. Cada módulo de información debe tener definidos quienes son los cargos políticos con acceso a dicha información.
Rector	Excmo. Sr. Rector de la Universidad

#### B.1.4 Cuadro de acceso a la información de estudiantes

Tipo información \ Clases usuarios	Universi- tarios	Personales mínimos	Particulares	Admvsos Básicos	Adminis- trativos	Acadé- micos	Docentes básicos	Docentes generales	Docentes específicos	Investi- gación	Económicos	Actividades	Salud	Sensibles
Todos	OP	NO	NO	np	np	NO	np	np	np	NO	NO	NO	NO	NO
Universidad	SI	NO	NO	np	np	NO	np	np	np	NO	NO	NO	NO	NO
PAS	SI	NO	NO	np	np	NO	np	np	np	NO	NO	NO	NO	NO
PDI	SI	NO	NO	np	np	NO	np	np	np	NO	NO	NO	NO	NO
Mis profesores	SI	NO	SI	np	np	SI	np	np	np	SI	NO	NO	NO	NO
Gestores de la información	SI	SI	SI	np	np	SI	np	np	np	SI	SI	SI	SI	SI
Decanos / Direc- tores de Centro	SI	NO	SI	np	np	SI	np	np	np	SI	NO	NO	NO	NO
Directores de Departamento	SI	NO	SI	np	np	SI	np	np	np	SI	NO	NO	NO	NO
Cargos universitarios	SI	SI	SI	np	np	SI	np	np	np	SI	NO	NO	NO	NO
Rector	SI	SI	SI	np	np	SI	np	np	np	SI	SI	SI	SI	SI

op: optativo

np: no procede

**B.1.5 Cuadro de acceso a la información personal de personal docente e investigador (PDI)**

Tipo información \ Clases usuarios	Universi- tarios	Personales mínimos	Particulares	Admvs Básicos	Adminis- trativos	Académicos	Docentes bá- sicos	Docentes ge- nerales	Docentes es- pecíficos	Investi- gación	Económicos	Actividades	Salud	Sensibles
Todos	op	NO	NO	NO	NO	NO	NO	NO	op	op	NO	NO	NO	NO
Universidad	SI	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO
PAS	SI	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO
PDI	SI	NO	NO	NO	NO	NO	SI	SI	NO	NO	NO	NO	NO	NO
Mis profesores	np	np	np	np	np	np	np	np	np	np	np	np	np	np
Gestores de la in- formación	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Decanos / Direc- tores de Centro	SI	SI	SI	SI	NO	NO	SI	SI	NO	NO	NO	NO	NO	NO
Directores de De- partamento	SI	SI	SI	SI	NO	NO	SI	SI	NO	NO	NO	NO	NO	NO
Cargos Universita- rios	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	NO	NO
Rector	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

**B.1.6 Cuadro de acceso a la información personal de personal de administración y servicios (PAS)**

Tipo información \ Clases usuarios	Universi- tarios	Personales mínimos	Particula- res	Admvs Básicos	Adminis- trativos	Acadé- micos	Docentes básicos	Docentes generales	Docentes específicos	Investi- gación	Económi- cos	Activid- ades	Salud	Sensibles
Todos	op	NO	NO	NO	NO	NO	np	np	np	op	NO	NO	NO	NO
Universidad	SI	NO	NO	NO	NO	NO	np	np	np	NO	NO	NO	NO	NO
PAS	SI	NO	NO	NO	NO	NO	np	np	np	NO	NO	NO	NO	NO
PDI	SI	NO	NO	NO	NO	NO	np	np	np	NO	NO	NO	NO	NO
Mis profesores	np	np	np	np	np	np	np	np	np	np	np	np	np	np
Gestores de la in- formación	SI	SI	SI	SI	SI	SI	np	np	np	SI	SI	SI	SI	SI
Decanos / Direc- tores de Centro	SI	SI	SI	SI	NO	NO	np	np	np	NO	NO	NO	NO	NO
Directores de De- partamento	SI	SI	SI	SI	NO	NO	np	np	np	NO	NO	NO	NO	NO
Cargos Universi- tarios	SI	SI	SI	SI	SI	SI	np	np	np	SI	NO	SI	NO	NO
Rector	SI	SI	SI	SI	SI	SI	np	np	np	SI	SI	SI	SI	SI

op: optativo

np: no procede

## **B.2. Procedimiento de comunicación interna de datos**

El acceso a datos de carácter personal no previsto en los cuadros de acceso anteriormente expuestos requerirá la autorización expresa del Gerente.

La realización de estas comunicaciones de datos deberá ser reflejada en el *Registro de Incidencias* de la Universidad de Zaragoza.

Éste procedimiento será de utilización también cuando por carencias en los sistemas de información un universitario no pueda acceder automáticamente a determinados datos personales aunque así esté previsto en los cuadros de acceso.

Las solicitudes de comunicación interna de datos deberán realizarse por escrito (ver anexo 1) y dirigidas al Gerente. Para agilizar y simplificar el proceso la Universidad podrá implantar sistemas telemáticos para la recepción de solicitudes siempre que tales sistemas aseguren la identificación del peticionario.

Las solicitudes deberán incluir, al menos, la siguiente información:

- Identificación del peticionario.
- Puesto, cargo o representación en función del que realiza la solicitud.
- Motivo de la solicitud.
- Datos solicitados.

## C. REGISTRO DE INCIDENCIAS

**C.1. Registro informatizado de incidencias. Gestión de incidencias**

Como mecanismo de coordinación, organización y gestión de los diferentes procesos y unidades que intervienen en el tratamiento de la información de que dispone la Universidad de Zaragoza, y para dar cumplimiento a lo dispuesto en los artículos 10 y 21 del RD 994/99 “Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal”, se establece un *Registro Informatizado de Incidencias* cuyas características y utilización se describen en los siguientes apartados.

Deberán anotarse obligatoriamente en el *Registro Informatizado de Incidencias*, al menos, los siguientes sucesos, así como todos aquellos previstos en la *normativa propia* de la Universidad, aprobada por resolución de 6 de junio de 2002 (BOA de 19 de junio):

- Cualquier incidencia de seguridad que afecte directa o indirectamente al fichero.
- Cualquier episodio que tenga como consecuencia la necesidad de recuperación de los datos a partir de las copias de seguridad de los mismos.
- Las solicitudes de acceso, rectificación o cancelación recibidas y su tramitación.
- Las solicitudes de cesión de datos así como todas las fases del procedimiento de cesión de los mismos que se produzca.
- Las solicitudes de identificadores de usuario, manteniendo actualizada en todo momento la relación de personas autorizadas de cada unidad.
- Informes mensuales de acceso.
- Las auditorias realizadas sobre el fichero así como las recomendaciones o sugerencias de los Responsables y Encargados Internos del Tratamiento y del Responsable y Encargados de seguridad.

Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma en el *Registro de Incidencias* del fichero o en su caso de la comunicación por escrito al responsable de seguridad o al encargado

interno del tratamiento. 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.

El *Registro Informático de Incidencias* tendrá restringido su acceso de acuerdo con el siguiente cuadro de permisos:

USUARIO	LEER INCIDENCIAS
Gerente	Todas
Gabinete Jurídico	Todas
Responsable Interno del tratamiento	Las suyas
Encargados Internos del Tratamiento	Las de su unidad
Responsable de seguridad	Todas
Encargados de seguridad	Todas
Usuarios	NO
Personal informático encargado de alguna tarea respecto del fichero	Las que les afecten

Sobre cada incidencia deberá constar, al menos, la siguiente información:

- Nombre de la persona que la anota.
- Fecha y hora de la anotación.
- Tipo de incidencia y descripción de la misma.
- Acciones a tomar sobre la incidencia y quién debe realizarlas.
- Indicador de si la incidencia permanece activa.

Los cuadros adjuntos muestran el formulario correspondiente a los tipos de anotaciones más usuales del registro.

**ANEXO 1. Modelo de comunicación interna de datos de carácter personal**

# SOLICITUD DE COMUNICACIÓN INTERNA DE DATOS DE CARÁCTER PERSONAL

NOMBRE Y APELLIDOS	DNI
CARGO O REPRESENTACIÓN EN FUNCIÓN DEL CUAL SOLICITA LOS DATOS	
<b>DATOS SOLICITADOS</b> Enumerar con precisión de qué tipo de personas necesita los datos (estudiantes de uno o varios centros, PDI catedráticos, PAS, etc.) y qué datos concretos precisa (nombre, apellidos, etc.)	
<b>MOTIVO DE LA SOLICITUD</b> Explique con claridad el motivo y la finalidad de esta petición	

El solicitante se compromete a guardar sigilo de los datos personales que reciba y a utilizarlos únicamente para el fin solicitado. Así mismo se compromete a destruir o devolver dichos datos (en todos los soportes en los que los posea) una vez cumplida la finalidad para la que los solicitó.

En \_\_\_\_\_ a \_\_ de \_\_\_\_\_ de 200\_\_  
(firma)

Ilmo Sr. Gerente de la Universidad de Zaragoza



**ANEXO 2. Pantallas del Registro Informatizado de Incidencias.**

**REGISTRO DE SOLICITUDES DE CESIÓN DE DATOS A TERCEROS**

RECEPCIÓN DE LA SOLICITUD  
Recibida por ..... Fecha y hora .....

Observaciones

DATOS DE LA SOLICITUD  
Solicitante .....  
Datos solicitados .....

Finalidad

INFORME DEL RESPONSABLE INTERNO DEL TRATAMIENTO

**RESOLUCIÓN DEL GERENTE**

Acceder  Denegar

Observaciones .....

Firma y fecha

**CONTROL DEL PROCESO**

Se ha remitido la carta con las *Condiciones de cesión de datos*  
 Se han recibido las *Condiciones* aceptadas y firmadas por el solicitante  
 Solicitar los datos al CCUZ  
 Registro interno

Precio público por costes advos: ..... Nº factura .....  Cobrado

Copia documental archivada

Proceso finalizado

**RESUMEN DE LOS DATOS PROCESADOS**

Fecha en la que se realiza la selección .....

Número total de registros obtenidos .....

Condiciones de búsqueda aplicadas .....

Observaciones .....

Figura 1. Registro de solicitudes de cesión de datos a terceros

<b>REGISTRO DE CESIÓN DE DATOS PARA LA PRESTACIÓN DE SERVICIOS</b>	
Anotado por .....	Fecha y hora .....
Finalidad de la cesión .....	
Empresa .....	
Fecha del contrato de prestación de servicios .....	
Datos transmitidos .....	
Fecha de envío .....	

Figura 2

<b>REGISTRO DE CESIÓN DE DATOS A OTRA ADMINISTRACIÓN</b>	
Anotado por .....	Fecha y hora .....
Finalidad de la cesión .....	
Organismo .....	
Datos transmitidos .....	
Fecha de envío .....	
Copia documental archivada .....	

Figura 3

<b>REGISTRO DE CESIÓN DE DATOS ORDENADA POR LEY</b>	
Anotado por .....	Fecha y hora .....
Finalidad de la cesión .....	
Organismo .....	
Datos transmitidos .....	
Fecha de envío .....	
Copia documental archivada .....	

Figura 4

**REGISTRO DE SOLICITUD DE COMUNICACIÓN DE DATOS A UNIDAD INTERNA**

**RECEPCIÓN DE LA SOLICITUD**

Recibida por ..... Fecha y hora .....

Observaciones

**DATOS DE LA SOLICITUD**

Solicitante .....

En representación de .....

Datos solicitados .....

Finalidad .....

**RESOLUCIÓN DEL GERENTE**

Acceder       Denegar

Observaciones .....

Firma y fecha

**CONTROL DEL PROCESO POR PARTE DEL RESPONSABLE DE SEGURIDAD**

Remisión de los datos ..... Fecha de remisión .....

Copia documental archivada

Proceso finalizado

**RESUMEN DE LOS DATOS PROCESADOS**

Fecha en la que se realiza la selección .....

Número total de registros obtenidos .....

Condiciones de búsqueda aplicadas .....

Observaciones

Figura 5

Se adjuntará a estas *Instrucciones de Servicio* el programa de software diseñado a estos efectos.



# BOUZ

*Boletín Oficial de la Universidad de Zaragoza*

Edita: Secretaría General  
Imprime: Servicio de Publicaciones  
Depósito legal: Z-619-2001  
ISSN: 1578-1585

Pedro Cerbuna, 12 – 50009 Zaragoza  
Tel. 976 76 10 07  
e-mail: [bouz@unizar.es](mailto:bouz@unizar.es)  
<http://wzar.unizar.es/bouz>