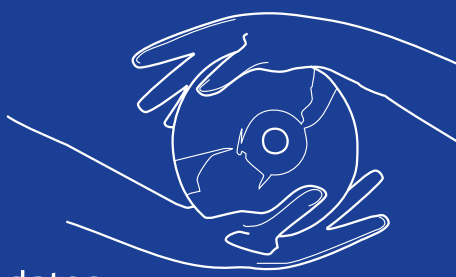

Reglamento de la UPV/EHU para la protección de datos de carácter personal

eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

Reglamento de la UPV/EHU para la protección de datos de carácter personal

Reglamento de la UPV/EHU para la protección de datos de carácter personal

Nuria Arregi (UPV/EHU)
Edurne Barañano (AVPD)
Joseba Eraña (UPV/EHU)
Sara Jorge (UPV/EHU)
Andoni Juaristi (UPV/EHU)
Ainoa Larrinaga (UPV/EHU)
Simón Mesanza (AVPD)

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

ISBN: 978-84-9860-198-5
Depósito legal: BI - 339-09

Fotocomposición: Ipar, S. Coop.
Zurbaran, 2-4 - 48007 Bilbao

Impresión: Gráficas Berriz, S.A.

ÍNDICE

PRESENTACIÓN

La profundización en los valores democráticos supone también una ampliación de las garantías en el ejercicio y salvaguarda de los derechos de la ciudadanía. Y en ese progresivo avance debe entenderse la regulación, cada vez más estricta, del uso que los poderes públicos pueden hacer de los datos de carácter personal.

La Universidad del País Vasco y la Agencia Vasca de Protección de Datos no son ajenas al compromiso de las administraciones para hacer un uso adecuado de esos materiales. Fruto de ese compromiso, en mayo de 2006 ambas entidades firmaron un convenio marco de colaboración que contemplaba, entre otras acciones, la elaboración de una guía de buenas prácticas. Como desarrollo de ese convenio, el Consejo de Gobierno de la UPV/EHU aprobó recientemente un Reglamento para la Protección de Datos de Carácter Personal, cuyo fin es armonizar la confidencialidad de éstos y la necesidad de que la universidad pueda llevar a cabo las funciones que le son propias.

Se trata, en definitiva, de que la universidad haga uso de los datos de carácter personal en la medida necesaria para desarrollar su actividad académica y administrativa, pero que lo haga al mismo tiempo con las mayores garantías de confidencialidad, para la salvaguarda del honor e intimidad de las personas.

La edición de este libro responde, además, al esfuerzo de ambas instituciones por extender el conocimiento de estas condiciones de uso, con el fin de que todas las personas que forman parte de la comunidad universitaria o que se relacionan con ella sean conscientes de sus derechos y puedan ejercerlos. Las disposiciones normativas suelen ser textos alejados de la vida diaria de la ciudadanía, por eso hemos pensado que difundir el contenido de estos derechos a través de nuevos soportes servirá para que más personas los conozcan.

Estamos seguros de que iniciativas como esta serán el mejor modo de garantizar una adecuada protección de los datos de carácter personal en las relaciones de la ciudadanía con la institución universitaria.

Iñaki Vicuña
Director de la AVPD

Iñaki Goirizelaia
Rector de la UPV/EHU

EXPOSICIÓN DE MOTIVOS

En los Centros, Departamentos e Institutos Universitarios de Investigación de la UPV/EHU, así como en el Rectorado y Vicerrectorados, y demás entes y servicios de la Universidad, se trata diariamente con datos de carácter personal. Estos datos pertenecen principalmente al alumnado, al personal docente e investigador y al personal de administración y servicios, pero también corresponden a personas ajenas a la Universidad como representantes de otras instituciones, trabajadores y trabajadoras de empresas subcontratadas y particulares objeto de investigaciones científicas.

Tal necesidad de la UPV/EHU de valerse de datos de personas que se relacionan con la misma y, a su vez, el fortalecimiento experimentado en los últimos años por la regulación relativa a la defensa de datos de carácter personal, hacen necesario idear los mecanismos necesarios para lograr un equilibrio entre la confidencialidad de los datos de carácter personal y el hecho de que la UPV/EHU, como universidad pública, pueda llevar a cabo las funciones que le son propias.

Por todo ello, se ha considerado conveniente aprobar este Reglamento, el cual además de contribuir a que la UPV/EHU cumpla con sus obligaciones en el ámbito de la protección de datos de carácter personal, aspira a convertirse en referente para el personal de la misma que trate con datos de carácter personal.

TÍTULO I.
DISPOSICIONES GENERALES

Artículo 1
Objeto

En el marco del respeto de lo establecido en la legislación relativa a la protección de datos de carácter personal y sus disposiciones de desarrollo, el presente Reglamento tiene como objeto regular el tratamiento de los datos de carácter personal en manos de la UPV/EHU protegiendo, en todo caso, el honor e intimidad de las personas titulares de dichos datos y garantizando, al mismo tiempo, el cumplimiento por parte de la Universidad de las funciones que le son propias en su calidad de entidad dedicada al servicio público de la educación superior mediante la docencia, la investigación y el estudio.

La UPV/EHU recaba datos de carácter personal para prestar el servicio público de la educación superior y su tratamiento lo realiza con respeto a la normativa aplicable.

Artículo 2
Ámbito de aplicación

Este Reglamento será de aplicación en la UPV/EHU a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de esos datos.

Artículo 3
Escenario legal

3.1. La normativa básica que la UPV/EHU debe respetar en el ámbito de la protección de datos de carácter personal es la siguiente:

a) Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

b) Artículo 18.4 de la Constitución española.
c) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).
d) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, RDLOPD).
e) Ley 2/2004, de 25 de febrero, de Ficheros de datos de Carácter Personal de Titularidad pública y de Creación de la Agencia Vasca de Protección de Datos.
f) Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos.

3.2. En el caso de que se produzcan cambios normativos, las referencias realizadas en este Reglamento a las disposiciones vigentes a su entrada en vigor serán consideradas realizadas a las que las sustituyan. Asimismo, este Reglamento será periódicamente actualizado en función de los nuevos requisitos normativos que puedan ser exigidos. La versión actualizada del Reglamento estará disponible en la página web de la Universidad (*www.ehu.es/babestu*).

La última versión del Reglamento y los supuestos concretos que se vayan regulando estarán disponibles en www.ehu.es/babestu.

Artículo 4
Definiciones

4.1. A la luz del presente Reglamento, se entenderán de la siguiente manera los conceptos básicos en materia de protección de datos de carácter personal indicados a continuación:

a) **Datos de carácter personal:** cualquier información numérica, alfabética, gráfica, fotográfica, acústica o del cualquier otro tipo concerniente a personas físicas identificadas o identificables.
b) **Persona identificable:** toda persona cuya identidad pueda determinarse directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.

c) **Datos especialmente protegidos:** datos que se refieren a ideología, religión, creencias, afiliación sindical, origen racial, salud, vida sexual o infracciones penales o administrativas.

d) **Datos de carácter personal relacionados con la salud:** las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

e) **Tratamiento de datos:** cualquier operación o procedimiento técnico, sea o no automatizado, que implique la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

f) **Fichero:** Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

g) **Fichero no automatizado:** todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos de carácter personal, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

Se denomina «Fichero» (automatizado o no) a todo conjunto organizado de datos de carácter personal, tanto si está almacenado en soporte informático como en papel.

h) **Afectado, afectada, interesada o interesado:** persona física titular de los datos que sean objeto de tratamiento.

i) **Consentimiento del interesado o interesada:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado o la interesada consienta el tratamiento de datos de carácter personal que le conciernen.

j) **Procedimiento de disociación:** todo tratamiento de datos de carácter personal de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

k) **Dato disociado:** Aquel que no permite la identificación de un afectado, afectada o interesada, interesado.

l) **Cesión o comunicación de datos:** tratamiento de datos que supone su revelación a una persona distinta de la interesada.

m) **Destinatario o cesionario:** la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

n) **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos de carácter personal por cuenta de la UPV/EHU, como consecuencia de la existencia de una relación jurídica que le vincula con la misma y delimita el ámbito de su actuación para la prestación de un servicio.

o) **Tercero:** la persona física o jurídica, autoridad pública o privada, u órgano administrativo distinto del afectado, afectada, interesada o interesado, de la persona Responsable Interno del fichero (definido en el artículo 5.4.b), del Encargado o Encargada del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del Responsable Interno del fichero o del Encargado o Encargada del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

p) **Fuentes accesibles al público:** aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, las guías de servicios de comunicaciones electrónicas en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación social.

q) **Cancelación:** Procedimiento en virtud del cual la persona responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

r) **Supresión, borrado:** la eliminación física de los datos de carácter personal cancelados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento de dichos datos.

s) **Usuario o Usuaria:** persona o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de una usuaria o un usuario físico. Los «perfiles de usuarios» consisten en accesos autorizados a un grupo de usuarios o usuarias.

4.2. A los efectos del presente Reglamento, los conceptos recogidos a continuación relacionados con las medidas de seguridad a adoptar serán entendidos de la siguiente manera:

a) **Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

b) **Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

c) **Recurso:** cualquier parte componente de un sistema de información.

d) **Accesos autorizados:** autorizaciones concedidas a un usuario o usuaria para la utilización de los diversos recursos.

e) **Identificación:** procedimiento de reconocimiento de la identidad de una usuaria o usuario.

f) **Autenticación:** procedimiento de comprobación de la identidad de un usuario o usuaria.

g) **Control de acceso**: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

h) **Contraseña:** información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o usuaria o en el acceso a un recurso.

i) **Fichero temporal:** fichero de trabajo creado por usuarios o procesos que es necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

j) **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

k) **Soporte:** objeto físico que almacena o contiene datos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

l) **Copia de respaldo:** copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
m) **Documentación:** todo escrito, señal, gráfico, sonido, dibujo, película, fotografía, cinta magnética, cinta mecanográfica, cassette, disco, CD-Rom, DVD, dispositivos externos de almacenamiento u otro medio físico en el que se haya registrado información.
n) **Transmisión de documentos:** cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

Artículo 5
Responsables

5.1. Todo el personal de la UPV/EHU que realice tratamientos de datos de carácter personal, de forma general o excepcional, deberá respetar la normativa al respecto. Los trabajadores y trabajadoras de la Universidad deberán preocuparse por conocer sus obligaciones y ser conscientes de las consecuencias, de carácter disciplinario o ante terceros, en el caso de actuar al margen de lo establecido en este Reglamento.

El Rector o Rectora es el último responsable de la aplicación de la normativa en materia de protección de datos de carácter personal en la Universidad. No obstante, todo el personal de la UPV/EHU que trate con datos de carácter personal responderá por sus actos.

5.2. Quienes tengan personal a su cargo, deberán formarlo debidamente en sus deberes en relación con la protección de datos de carácter personal, prestando especial atención a las nuevas personas que se incorporen a sus equipos.

5.3. La UPV/EHU asume su responsabilidad corporativa en relación con el deber de garantizar una protección de datos de carácter personal eficaz y válida en el ámbito de la Universidad en el marco de lo establecido en la normativa relativa a la protección de datos de carácter personal. En consecuencia, la UPV/EHU planificará periódicamente acciones informativas y formativas dirigidas a su personal, y de una manera preferente a quienes traten con más datos de carácter personal o datos especialmente protegidos.

5.4. El **Rector o Rectora** será el máximo o la máxima responsable de la efectiva aplicación de la normativa en materia de protección de datos de carácter personal por parte de la UPV/EHU, y **Responsable último de todos los fi-**

cheros declarados por la Universidad. Asimismo, en la UPV/EHU se identifican las siguientes figuras con responsabilidad en la protección de datos de carácter personal:

a) **Responsable de Seguridad LOPD**: persona encargada de definir y velar por el cumplimiento de la estrategia global en materia de seguridad de la información de la UPV/EHU y, especialmente, la correcta adecuación de la misma a lo establecido en la normativa relativa a la protección de datos de carácter personal. Entre sus funciones estará la de canalizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, las revocaciones de consentimiento y las impugnaciones de valoraciones que puedan presentarse.

b) **Responsable Interno de fichero:** persona que, por delegación del Rector o Rectora, decide sobre la finalidad, contenido y el tratamiento del o de los ficheros que le sean asignados. La persona Responsable Interno del fichero cumplirá con las funciones asignadas por la normativa en materia de protección de datos de carácter personal y el presente Reglamento a la persona «Responsable del fichero o tratamiento».

c) **Comité de Seguridad Informática y Gestión Documental:** órgano que realiza la función de «***Responsable de Seguridad***» (según definición del RDLOPD) de todos los ficheros de la UPV/EHU, y cuya función consiste en coordinar y controlar las medidas de seguridad aplicables a los citados ficheros.

La función de la figura del «Responsable de Seguridad» previsto en la ley, la realiza en la UPV/EHU el «Comité de Seguridad Informática y Gestión Documental».

d) **Comisión para la Protección de Datos:** órgano encargado de llevar a cabo la coordinación y control de la efectiva implantación del presente Reglamento y establecer las pautas generales de actuación de la UPV/EHU en cuestión de protección de datos.

e) **Coordinador o Coordinadora de la protección de datos de carácter personal de Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u otro organismo universitario:** el máximo o la máxima persona responsable del Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u organismo universitario asumirá la responsabilidad de difundir, implantar y garantizar la efectiva aplicación de

la normativa relativa a la protección de datos de carácter personal de la Universidad en el ámbito que le corresponda, en coordinación y colaboración con el resto de responsables en materia de protección de datos de carácter personal de la Universidad, y pudiendo designar a su vez a otras personas para estar tareas sin que ello implique una delegación de su responsabilidad.

5.5. En el Título IV del presente Reglamento se concretan las previsiones respecto a los responsables universitarios en materia de protección de datos.

TÍTULO II.
TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CAPÍTULO 1

Recogida de datos de carácter personal

Artículo 6
Modo de recabar y tratar los datos

6.1. Los datos de carácter personal deberán ser tratados de forma leal y lícita, por lo que se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

6.2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas.

6.3. La UPV/EHU tendrá presente, en todo momento, el principio de que los datos de carácter personal son propiedad de las personas a las que se refieren y no los solicitará ni hará uso de ellos salvo para aquellas finalidades para las que esté facultada debidamente.

Artículo 7
Información sobre el uso y la finalidad

7.1. Los formularios de recogida de datos, tanto en papel como en pantalla, deberán incluir de modo expreso, preciso e inequívoco la siguiente información:

a) la existencia de un fichero o tratamiento de datos de carácter personal, la finalidad de la recogida de éste y los destinatarios de la información;
b) en su caso, los cesionarios o categorías de cesionarios de los datos, delimitados al menos por el tipo de actividad, determinada y explícita, a la que los mismos se dediquen;

Cada persona es propietaria de sus datos de carácter personal, por lo que la Universidad únicamente puede recabarlos de forma leal y lícita, y sólo puede utilizarlos para fines determinados, explícitos y legítimos.

c) el carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas;
d) las consecuencias de la obtención de los datos o de la negativa a suministrarlos;
e) la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y del órgano ante el que se ejercitan tales derechos.
f) la identidad y dirección de la persona Responsable del fichero o tratamiento.

7.2. No será necesaria la inclusión del contenido de los apartados c) y d) anteriores, en el caso de que dicha información pueda deducirse de la naturaleza de los datos de carácter personal que se solicitan o de las circunstancias en que se recaban.

7.3. Con el fin de llevar el derecho de información a su máxima expresión, la Universidad informará de la existencia del presente Reglamento cuando recoja datos de carácter personal a través de formularios, indicando su ubicación en Internet en la web de la Universidad y en el de la Agencia Vasca de Protección de Datos para su consulta.

7.4. Cuando los datos de carácter personal no hayan sido recabados de la interesada o interesado, éste deberá ser informado por la UPV/EHU, dentro de los tres meses siguientes al momento de registro de los datos, de forma expresa, precisa e inequívoca, salvo que ya hubiera sido informado con anterioridad, sobre:

a) el contenido del tratamiento;
b) la procedencia de los datos;
c) la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y
d) la identidad y dirección de la persona «Responsable de fichero o tratamiento».

7.5. En el *Anexo I.M I* del presente Reglamento se recoge la cláusula informativa a introducir en los formularios donde se recaben datos de terceros. Se advierte que el contenido de la cláusula informativa es de carácter mínimo y, por lo tanto, en algunos casos será necesario completarla con otra serie de cuestiones como fórmulas de solicitud de autorización para futuras cesiones de datos por parte de la Universidad.

Los formularios que recaben datos de carácter personal deben contener la cláusula informativa correspondiente.

Artículo 8
Calidad de los datos

8.1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

8.2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

8.3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán rectificados o cancelados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, sin perjuicio del ejercicio de los derechos por parte de las interesadas o los interesados reconocidos en los artículos 14, 15, 16 y 17 del presente Reglamento.

Cuando los datos hubieran sido comunicados previamente, la persona Responsable del fichero o tratamiento deberá notificar al cesionario o cesionaria, en el plazo de diez días, la rectificación o cancelación efectuada. En el plazo de diez días desde la recepción de la notificación, la cesionaraia o el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación o cancelación notificada. Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado.

No se puede recabar más datos que los estrictamente necesarios, ni usarlos para fines diferentes a aquellos para los que hubiesen sido recabados.

Artículo 9
Tratamiento con fines estadísticos, históricos o científicos

9.1. No se considerará incompatible, a los efectos previstos en el artículo 8.2 del presente Reglamento, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos. Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de

mayo, reguladora de la Función Estadística Pública, la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y la Ley 13/1986, de 14 de abril, de Fomento y Coordinación General de la Investigación Científica y Técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

9.2. La Agencia Vasca de Protección de Datos podrá, previa solicitud de la persona Responsable del fichero o tratamiento y conforme al procedimiento establecido en la Sección Segunda del Capítulo VII del Título IX del RDLOPD, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10
Conservación y cancelación de los datos

10.1. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación y posterior supresión o borrado.

10.2. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato.

10.3. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión o borrado de los datos.

10.4. La supresión o borrado supone la eliminación física de los datos de carácter personal cancelados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento de dichos datos.

10.5. En todo caso, habrá que respetar lo establecido por la UPV/EHU en relación con la conservación y supresión de los datos en documentos y soportes.

Cuando los datos de carácter personal dejen de ser necesarios o pertinentes para la finalidad para la que hubiesen sido recabados o registrados, serán cancelados y, en su caso, suprimidos o borrados.

Artículo 11
Consentimiento de la persona

11.1. Salvo que la ley disponga otra cosa, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado. La obtención de dicho consentimiento se realizará siguiendo alguna de las fórmulas indicadas en el artículo 12 del presente Reglamento.

11.2. No obstante, la Universidad no tendrá la obligación de solicitar su consentimiento a las personas titulares de los datos de carácter personal de los que quiera valerse cuando desee utilizarlos en alguno de los siguientes supuestos:

a) los datos de carácter personal se recogen para el ejercicio de las funciones propias de la Universidad en el ámbito de sus competencias;
b) los datos de carácter personal se refieren a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y son necesarios para su mantenimiento o cumplimiento;
c) el tratamiento de los datos de carácter personal tiene por finalidad proteger un interés vital del interesado en los términos del artículo 7.6 de la LOPD;
d) los datos figuran en fuentes accesibles al público y su tratamiento es necesario para la satisfacción del interés legítimo perseguido por la UPV/EHU o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado o interesada.

Para llevar a cabo tratamientos de datos de carácter personal es necesario obtener el consentimiento del afectado o afectada, salvo en los supuestos indicados en el artículo 11.

11.3. Respecto a los datos de carácter personal relativos a la salud, vida sexual u origen racial, estos sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general así lo disponga una ley o el interesado o la interesada consienta expresamente. Las y los profesionales de la UPV/EHU directamente relacionados con la salud de los trabajadores podrán tratar los datos de carácter personal relativos a la salud de las personas que a ellos acudan, de acuerdo con lo dispuesto en la normativa vigente en materia de sanidad y de protección de la salud y prevención de riesgos laborales.

11.4. El tratamiento de datos relativos a ideología, religión, creencias y afiliación sindical, requiere el consentimiento expreso y por escrito del interesado o interesada. En el caso de que se recabasen datos relativos a la ideología, religión o creencias de la interasada o del interesado, éste será advertido de su derecho a no consentir el tratamiento de tales datos.

11.5. Una vez dado el consentimiento, éste podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. La revocación del consentimiento podrá realizarse mediante escrito dirigido a la persona «Responsable de Seguridad LOPD» manifestando tal decisión y éste, tras haber consultado al correspondiente Responsable de fichero o tratamiento, deberá responder expresamente en el plazo de diez días desde la recepción de la solicitud de revocación del consentimiento, materializando, en su caso, tal revocación dentro del mismo plazo. Si los datos para cuyo tratamiento se revoca el consentimiento hubieran sido comunicados previamente, la UPV/EHU deberá notificar la revocación del consentimiento efectuada a quien se hayan comunicado en el caso de que se mantenga el tratamiento por este último. El modelo de revocación del consentimiento se recoge en el *Anexo I.M II*. También es posible revocar el consentimiento ejerciendo el derecho de cancelación previsto en el artículo 16 del presente Reglamento.

El consentimiento podrá revocarse en cualquier momento mediante escrito dirigido a la persona «Responsable de Seguridad LOPD».

Artículo 12
Fórmulas para recabar el consentimiento

12.1. La fórmula de autorización expresa para el tratamiento de datos figura como *Anexo I.M III* del presente Reglamento.

12.2. Asimismo, en determinados supuestos como por ejemplo en el caso de que la persona Responsable del fichero o tratamiento solicite el consentimiento del afectado o afectada durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual que se pretende acordar, se podrá permitir a la afectada o afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos posibilitándole la marcación de una

casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

La UPV/EHU contempla varias formas de recabar el consentimiento:
a) expresamente;
b) mediante marcación de casilla;
c) no oponiéndose al tratamiento.

12.3. En aquellos supuestos en los que el consentimiento expreso no sea exigido de manera imperativa por una ley, la persona Responsable del fichero o tratamiento podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la LOPD y 12.2 del RDLOPD, y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. En todo caso, será necesario que la persona Responsable del fichero o tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado o interesada.

Deberá facilitarse a la interesada o interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerarán ajustados al presente Reglamento el que tal negativa pueda efectuarse mediante correo electrónico o su envío en sobre previamente facilitado por la Universidad con el franqueo pagado u otra modalidad postal.

Cuando se solicite el consentimiento del interesado o de la interesada a través de este último procedimiento, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

CAPÍTULO 2

Derechos de los interesados e interesadas

Artículo 13
Solicitudes de acceso, rectificación, cancelación y oposición

13.1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos, y serán ejercidos por la interesada o interesado. Tales derechos se ejercitarán:

a) Por el afectado o afectada, acreditando su identidad.
b) Cuando la afectada o afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.
c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad de la persona representada mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquélla por cualquier medio válido en derecho

Los derechos fundamentales de toda persona en relación con sus datos de carácter personal son conocidos como derechos ARCO:
A- Acceso
R- Rectificación
C- Cancelación
O- Oposición

que deje constancia fidedigna (por ejemplo, poder notarial) o mediante declaración en comparecencia personal del interesado o interesada.

Para ejercer sus derechos, el interesado o interesada debe acreditar su identidad. No se atenderán solicitudes de datos telefónicas, ni las realizadas por los padres y madres del alumnado sin la obtención de la debida representación.

13.2. Será imprescindible que la interesada o interesado acredite su identidad. Por esta razón, no serán atendidas las solicitudes de ejercicio de estos derechos que se efectúen por teléfono o cualquier otro medio que no permita acreditar la identidad de la interesada o interesado.

13.3. Los padres, madres, tutores o cualquier otro tercero, no tendrán acceso al expediente académico o a cualquier otro dato personal de sus hijos, hijas o personas queridas vinculadas con la UPV/EHU, salvo en los supuestos expresamente aceptados por el presente artículo.

Esta imposibilidad se extiende a los datos de carácter personal de la persona fallecida. No obstante, las personas vinculadas al fallecido o fallecida, por razones familiares o de hecho, podrán dirigirse a la persona «Responsable de Seguridad LOPD» con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos. La persona «Responsable de Seguridad LOPD» comunicará la información facilitada a la persona Responsable del fichero o tratamiento afectado.

13.4. Los derechos de acceso, rectificación, cancelación y oposición se ejercerán mediante escrito dirigido a la persona «Responsable de Seguridad LOPD», a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La persona

Se habilitarán formularios específicos para ejercer los derechos ARCO, que estarán a disposición de la comunidad universitaria en los registros y en www.ehu.es/babestu.

«Responsable de Seguridad LOPD» se encargará de hacer llegar las solicitudes recibidas a las personas Responsables de fichero o tratamiento implicados. El anterior escrito contendrá las siguientes determinaciones y requisitos:

a) Nombre y apellidos del interesado o interesada; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa de la afectada o afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.
b) Petición en que se concreta la solicitud.
c) Domicilio a efectos de notificaciones, fecha y firma de la persona solicitante.
e) Documentos acreditativos de la petición que formula, en su caso.

13.5. El interesado o interesada deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud. Con objeto de facilitar el ejercicio de estos derechos, en el Registro General de la Universidad y sus Registros auxiliares, así como en la página web de la Universidad, se pondrán a disposición de las personas interesadas los correspondientes formularios.

13.6. En el caso de que la solicitud no reúna los requisitos especificados en el apartado cuarto de este artículo, la persona «Responsable de Seguridad LOPD», siguiendo las indicaciones de la persona Responsable del fichero o tratamiento, deberá solicitar la subsanación de los mismos.

13.7. La UPV/EHU articulará los mecanismos necesarios para que las personas de su organización que tienen acceso a datos de carácter personal puedan informar al afectado o afectada respecto al procedimiento a seguir para el ejercicio de sus derechos.

13.8. Cuando los afectados o afectadas ejerciten sus derechos ante la persona Encargada del tratamiento, ésta deberá dar traslado de la solicitud a la persona «Responsable de Seguridad LOPD», a menos que se prevea expresamente que el Encargado atenderá, por cuenta de la persona responsable, las solicitudes de ejercicio por los afectados o afectadas de sus derechos de acceso, rectificación, cancelación u oposición.

Mediante el derecho de acceso, cada persona puede conocer los datos que la UPV/EHU tiene sobre ella.

Artículo 14
Derecho de acceso

14.1. El derecho de acceso es el derecho de la afectada o afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

14.2. Al ejercitar el derecho de acceso, la interesada o interesado podrá optar, al formular su solicitud, por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

a) Presencialmente mediante visualización en pantalla.
b) Escrito, copia o fotocopia remitida por correo.
c) Correo electrónico u otros sistemas de comunicaciones electrónicas.
d) Cualquier otro procedimiento que sea adecuado a la configuración o implantación material del fichero o la naturaleza del tratamiento.

No obstante, los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado o afectada sea gratuito y asegure la comunicación escrita si ésta así lo exige.

14.3. La solicitud de acceso se resolverá en el plazo máximo de un mes a contar desde la recepción de la solicitud. Si la solicitud fuera estimada pero no acompañase en la comunicación la información solicitada, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

14.4. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios o cesionarias de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

14.5. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que la persona interesada acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

14.6. Existe un modelo de formulario para el ejercicio del derecho de acceso en el *Anexo I.M IV*.

Artículo 15
Derecho de rectificación

15.1. Cuando el titular o la titular de los datos tuvieran constancia de que sus datos de carácter personal tratados en un fichero son inexactos o incompletos, podrá solicitar a la UPV/EHU la rectificación de los mismos. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En el caso de que los datos de carácter personal que disponga la Universidad sean inexactos o incompletos, su titular puede solicitar su rectificación.

15.2. La Universidad hará efectivo el derecho de rectificación del interesado en el plazo de diez días hábiles.

15.3. Serán rectificados los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la LOPD y, en particular, cuando tales datos resulten inexactos o incompletos.

15.4. Si los datos rectificados hubieran sido cedidos previamente, se deberá comunicar la rectificación efectuada al cesionario o cesionaria, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar los datos.

15.5. Existe un modelo de formulario para el ejercicio del derecho de rectificación en el *Anexo I.M V*.

El ejercicio del derecho de cancelación dará lugar al bloqueo de los datos inadecuados o excesivos y, en su caso, a su supresión o borrado.

Artículo 16
Derecho de cancelación

16.1. El ejercicio del derecho de cancelación dará lugar al bloqueo de los datos inadecuados o excesivos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

16.2. En la solicitud de cancelación, el interesado o interesada deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso. La afectada o afectado podrá valerse de la solicitud de cancelación para revocar su consentimiento.

16.3. La UPV/EHU hará efectivo el derecho de cancelación de la interesada o interesado en el plazo de diez días hábiles.

16.4. En los casos en que, siendo procedente la supresión de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, la persona Responsable del fichero o tratamiento procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización. Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

16.5. Si los datos cancelados hubieran sido cedidos previamente, se deberá comunicar la cancelación efectuada al cesionario o cesionaria, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a cancelar los datos.

16.6. Existe un modelo de formulario para el ejercicio del derecho de cancelación en el *Anexo I.M VI*.

Artículo 17
Derecho de oposición

17.1. El derecho de oposición es el derecho del afectado o afectada a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una ley no disponga lo contrario.

b) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado o afectada y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 del RDLOPD.

En determinados supuestos el titular de los datos puede negarse a que se lleve a cabo el tratamiento de sus datos de carácter personal.

17.2. La UPV/EHU deberá excluir del tratamiento los datos relativos a la afectada o afectado que ejercite su derecho de oposición o denegar motivada-

mente la solicitud del interesado o interesada en el plazo de diez días hábiles a contar desde la recepción de la solicitud.

17.3. Existe un modelo de formulario para el ejercicio del derecho de oposición en el *Anexo I.M VII*.

Artículo 18
Tramitación de las solicitudes de acceso, rectificación, cancelación y oposición

18.1. La solicitud de acceso, rectificación, cancelación u oposición será contestada por la persona «Responsable de Seguridad LOPD», en función de lo indicado por la persona Responsable de fichero o tratamiento con independencia de que figuren o no datos de carácter personal del interesado en los ficheros de acuerdo con lo dispuesto a continuación, mediante notificación administrativa. En el caso de que no se disponga de datos de carácter personal de los interesados o interesadas, tal circunstancia será comunicada al interesado.

18.2. No se exigirá contraprestación alguna por el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

18.3. Corresponderá al Servicio Jurídico de la UPV/EHU el asesoramiento a la persona Responsable de Seguridad LOPD y Responsable del fichero o tratamiento sobre la homogeneización y fijación de los criterios aplicables en la atención a los derechos del interesado. A tal efecto, la persona Responsable de Seguridad LOPD remitirá al Servicio Jurídico, junto con la documentación necesaria, aquellas solicitudes de acceso, rectificación, cancelación u oposición, que por sus características particulares o por las cuestiones en ellos planteadas, se considere que deben ser objeto de análisis jurídico específico. El Servicio Jurídico recabará los informes que estime oportunos y realizará una propuesta de resolución en el plazo más breve posible, y en cualquier caso de tal modo que se puedan cumplir los plazos de respuesta asumidos por la Universidad.

El ejercicio de los derechos ARCO es gratuito.

18.4. Se rechazará la solicitud en los siguientes casos:

a) En los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa.

b) Cuando el solicitante sea una persona distinta del interesado o interesada o de su representante, de acuerdo con lo dispuesto en el artículo 13.1 del presente Reglamento.
c) En el caso o en el caso del derecho de acceso, cuando una ley o norma de derecho comunitario de aplicación directa impida revelar a los afectados el tratamiento de los datos a los que se refiera el acceso. Asimismo, cuando se haya ejercitado tal derecho de acceso en los últimos doce meses, salvo que se acredite un interés legítimo.
d) En el caso del derecho de rectificación, cuando no se indique el dato que es erróneo y la corrección que deba realizarse.
e) En el caso del derecho de cancelación, cuando se pueda causar un perjuicio a intereses legítimos de la interesada o interesado o de terceros, cuando exista una relación contractual, cuando deban gestionarse pagos y cobros, o cuando su mantenimiento sea preciso para el adecuado cumplimiento de los fines de la UPV/EHU.

18.5. Si solicitado el acceso, la rectificación, la cancelación u oposición al tratamiento, se considera que no procede acceder a la solicitud del interesado o interesada, así se le comunicará de forma motivada. En todo caso, la UPV/EHU deberá justificar su denegación e informar al afectado de su derecho a recabar la tutela de la Agencia Vasca de Protección de Datos, conforme a lo dispuesto en el artículo 18 de la LOPD.

La UPV/EHU responderá en el plazo de un mes a las solicitudes de acceso, y en el plazo de diez días hábiles a las de rectificación, cancelación u oposición. En caso de denegación de tales solicitudes, la Universidad le informará al afectado o afectada de su derecho a recabar la tutela de la Agencia Vasca de Protección de Datos.

18.6. La UPV/EHU deberá dar respuesta a todas las solicitudes y conservará la acreditación del cumplimiento del mencionado deber; no obstante, en el caso de silencio administrativo en los plazos fijados, se entenderá que la solicitud ha sido rechazada.

18.7. Desde el momento en que transcurra un mes desde el ejercicio del derecho de acceso, o diez días hábiles en el caso de los derechos de rectificación, cancelación y oposición, sin que el interesado o interesada haya obtenido ninguna respuesta o cuando ésta sea negativa o no satisfactoria, el interesado podrá ejercitar su derecho de tutela ante la Agencia Vasca de Protección de Datos.

Artículo 19
Impugnación de valoraciones

Las personas interesadas tendrán derecho a impugnar valoraciones basadas en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad ante la persona Responsable de Seguridad LOPD, el cual se encargará de encauzar la solicitud a los Responsables de fichero o tratamiento afectados.

CAPÍTULO 3

Comunicación de datos de carácter personal

Artículo 20
Deber de secreto

20.1. Toda persona que intervenga en cualquier fase del tratamiento de los datos de carácter personal de la UPV/EHU está obligada al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar su relación con la Universidad.

20.2. El incumplimiento del deber de secreto será sancionado de conformidad con lo previsto en la legislación vigente y traerá consigo las responsabilidades disciplinarias y, en su caso ante terceros, que se establezcan.

El incumplimiento del deber de secreto en el tratamiento de datos de carácter personal podrá acarrear responsabilidades disciplinarias.

Artículo 21
Obligaciones en las comunicaciones de datos

21.1. Salvo en los casos expresamente previstos e indicados en el artículo 23 del presente Reglamento, los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas de la UPV/EHU y del cesionario con el previo consentimiento de la persona interesada respetando, en todo caso, lo establecido en el artículo 11 del presente Reglamento.

21.2. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite a la persona in-

teresada no le permita conocer el tipo de datos cuya cesión se autoriza, la finalidad a la que se destinarán dichos datos, o el tipo de actividad de aquél a quien se pretenden comunicar.

21.3. El consentimiento para la comunicación de los datos de carácter personal tiene carácter revocable, por lo que, en caso de producirse siguiendo lo establecido en el artículo 11.5 del presente Reglamento, se deberá comunicar de inmediato la revocación a los cesionarios instándoles a que cesen en el tratamiento de los datos del interesado.

21.4. Aquél 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 LOPD.

21.5. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Si se facilita la información de tal forma que es imposible identificar a la persona a la que se refiere (datos disociados), puede ser cedida sin consentimiento previo.

Artículo 22
Cesiones que requieren el consentimiento del afectado o afectada

22.1. En el caso de que una entidad externa solicite a la UPV/EHU la cesión de datos de carácter personal en sus manos para un fin que la Universidad considere de interés, se deberá proceder a la tramitación del correspondiente convenio respetando lo establecido en la normativa universitaria aplicable. En el *Anexo II. SC IV* del presente Reglamento se profundiza en este supuesto.

En la tramitación del convenio, se solicitarán informes a la persona «Responsable de Seguridad LOPD» y a la persona Responsable del fichero o tratamiento, los cuales serán vinculantes. Para que se pueda llevar a cabo la cesión, la persona Responsable del fichero o tratamiento deberá confirmar en su informe que las personas cuyos datos se solicitan han dado previamente el consentimiento para la cesión y, si no lo han hecho, solicitar dicha autorización. La solicitud del consentimiento se realizará en el marco de lo establecido en el artículo 12 del presente Reglamento.

La persona Responsable del fichero o tratamiento procederá al registro de las cesiones de datos realizadas, con el fin de garantizar el efectivo futuro ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los interesados o

interesadas. Asimismo, las cesiones realizadas serán reflejadas en el correspondiente Registro de entradas y salidas del Documento de Seguridad del fichero.

La UPV/EHU podrá atender solicitudes de cesión de datos a entidades externas mediante la tramitación de un convenio. No obstante, la Universidad puede hacerse cargo de la distribución de la información si la acción es de su interés.

22.2. Como salvedad al procedimiento establecido en los apartados anteriores, si se recibe una solicitud de datos por parte de una entidad externa y la UPV/EHU considera de interés colaborar en la divulgación de determinada información facilitada por la entidad externa (interés el cual siempre tendrá que estar relacionado con los fines de la UPV/EHU según sus Estatutos), la Universidad podrá llevar a cabo dicha distribución y correr con los gastos.

La unidad organizativa de la UPV/EHU implicada (Rectorado, Vicerrectorados, Gerencia, Centros, Institutos y Cátedras), tras la correspondiente aprobación de la iniciativa por su máximo responsable, solicitará el permiso correspondiente a la persona Responsable de Seguridad LOPD. Una vez de haber recibido la autorización por escrito de la persona «Responsable de Seguridad LOPD», la unidad organizativa interesada se encargará del envío de la información facilitada por la entidad externa, la cual irá introducida obligatoriamente por un escrito de presentación de la Universidad que justifique el interés de dicho envío.

El medio prioritario de distribución será el correo electrónico. Tan sólo en supuestos excepcionales, debidamente justificados en la solicitud que se realice a la persona «Responsable de Seguridad LOPD», se procederá al envío por correo postal y en tal caso, los gastos serán asumidos por la propia Universidad.

Asimismo, se podrán habilitar en la web de la Universidad lugares en los que se pueda colocar información no directamente relacionada con la Universidad pero de interés para la comunidad universitaria.

Artículo 23
Cesiones que no requieren el consentimiento del afectado o afectada

23.1. Al margen de lo establecido en los artículos anteriores, no se requerirá el previo consentimiento de la afectada o afectado, de acuerdo con lo establecido en los artículos 11 y 21 de la LOPD, cuando la Universidad haya sido reque-

rida para ceder o desee facilitar dichos datos a un tercero en los siguientes supuestos:

a) La cesión está autorizada por una norma con rango de ley o una norma de derecho comunitario.
b) Se trate de datos recogidos de fuentes accesibles al público y su tratamiento es necesario para la satisfacción del interés legítimo perseguido por la UPV/EHU o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
c) El tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales, o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) La cesión se produzca entre Administraciones públicas en los tres siguientes casos: cuando la cesión tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos; cuando sean datos de carácter personal que una Administración pública haya obtenido o elaborado con destino a otra; y cuando la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.
f) Cuando la cesión se efectúe previo procedimiento de disociación, es decir, de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

La UPV/EHU únicamente puede ceder los datos, sin el consentimiento del titular, en los supuestos previstos en la presente normativa y cuando una ley o norma de derecho comunitario lo autorice.

23.2. En tales casos, las cesiones se llevarán a cabo mediante la supervisión de la persona Responsable de Seguridad LOPD y la persona Responsable del fichero o tratamiento. En caso de duda, será obligatorio consultar a la persona Responsable de Seguridad LOPD.

Artículo 24
Transferencia internacional de datos

24.1. A la luz del presente Reglamento, se entiende como transferencia internacional de datos, el tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (compuesto por los países miembros por la Unión Europea, Liechtenstein, Noruega e Islandia) y Suiza, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta de la persona Responsable del fichero o tratamiento.

Se producen transferencias internacionales de datos en las transmisiones de información a países que no pertenecen al Espacio Económico Europeo.

24.2. Podrán realizarse transferencias internacionales de datos de carácter personal con destino a países que proporcionen un nivel de protección equiparable a la LOPD, en función de lo establecido en los artículos 67, 68 y 69 de la RDLOPD. De otro modo, se deberá obtener la autorización previa del Director o Directora de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen las garantías adecuadas.

24.3. Lo dispuesto en el apartado anterior no será de aplicación si la persona afectada hubiera dado su consentimiento inequívoco a la cesión, cuando la cesión fuera necesaria para la ejecución de un servicio o contrato en interés del afectado, o en cualquiera de los restantes supuestos previstos en el artículo 34 de la LOPD.

CAPÍTULO 4

Encargado del tratamiento

Artículo 25
Relaciones entre la persona Responsable Interna del fichero y el Encargado del tratamiento

25.1. El acceso a los datos por parte de un Encargado o Encargada del tratamiento que resulte necesario para la prestación de un servicio no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la LOPD y en el presente Capítulo.

El servicio prestado por el Encargado o Encargada del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado o afectada.

25.2. Cuando la persona Responsable del fichero o tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos de carácter personal sometido a lo dispuesto en este Capítulo deberá velar por que el Encargado o Encargada del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

25.3. En el caso de que el Encargado o Encargada del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el artículo 12.2 de la LOPD, será considerado, también, la persona Responsable del fichero o tratamiento, respondiendo de las infracciones en que hubiera incurrido.

No obstante, la persona encargada del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa de la persona Responsable del fichero o tratamiento, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 26
Posibilidad de subcontratación de los servicios

26.1. El Encargado o Encargada del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado la persona Responsable del fichero o tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta de la persona Responsable del fichero o tratamiento.

Para que la persona encargada del tratamiento subcontrate servicios a un tercero, necesita la previa autorización de la UPV/EHU. Esta autorización se obtiene de la persona «Responsable del fichero o tratamiento».

26.2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación, sin necesidad de nueva autorización, siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato suscrito entre la Universidad y el Encargado del tratamiento los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el Encargado o Encargada del tratamiento comunique a la persona responsable de la Universidad los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones de la persona Responsable del fichero o tratamiento.

26.3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el con-

trato, dicha necesidad será sometida a la consideración de la persona Responsable del fichero o tratamiento. Este último decidirá si aceptar o rechazar la solicitud y, en su caso, llevará a cabo los trámites necesarios para que la empresa a subcontratar cumpla, al menos, con los compromisos asumidos por la empresa contratada.

Artículo 27
Conservación de los datos por el Encargado del tratamiento

27.1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos a la persona Responsable del fichero o tratamiento o al encargado o encargada que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando la persona Responsable del fichero o tratamiento dicha conservación.

27.2. El Encargado o Encargada del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con la persona Responsable del fichero o tratamiento.

TÍTULO III.
REQUISITOS FORMALES RELATIVOS A LOS FICHEROS

Artículo 28.
Creación, modificación y supresión de ficheros

28.1. La decisión de creación, modificación o supresión de ficheros de la UPV/EHU será adoptada por su Consejo de Gobierno y la resolución correspondiente será publicada en el Boletín Oficial del País Vasco. Una vez publicada tal Resolución, ésta será notificará a la Agencia Vasca de Protección de Datos para su inscripción en el Registro de Protección de Datos de Euskadi.

La creación, modificación o supresión de ficheros la realizará el Consejo de Gobierno de la UPV/EHU y se publicará en el BOPV para su general conocimiento.

28.2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) la identificación del fichero, indicando su denominación, así como la descripción de su finalidad y usos previstos;
b) las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;
c) el procedimiento de recogida de los datos de carácter personal;
d) la estructura básica del fichero;
e) la descripción de los tipos de datos de carácter personal incluidos en el mismo;
f) las cesiones de datos de carácter personal previstas;
g) las transferencias de datos que se prevean a países terceros, en su caso;
h) la UPV/EHU como Responsable de fichero o tratamiento;
i) el Rectorado de la Universidad como la unidad donde se puede ejercitar los derechos de acceso, rectificación, cancelación y oposición; y
j) las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

28.3. Cuando una unidad de la Universidad necesite por razones de servicio recabar datos distintos a los mencionados en los ficheros registrados de la UPV/EHU inscritos ante la Agencia Vasca de Protección de Datos, dicha unidad realizará una solicitud a la persona Responsable de Seguridad LOPD requiriendo tal posibilidad mediante escrito motivado. En caso de reunir todas las condiciones exigidas por la ley, sus disposiciones de desarrollo y este Reglamento, la persona Responsable de Seguridad LOPD, junto con el Servicio Jurídico de la Universidad, llevarán a cabo los trámites precisos para la modificación de los ficheros inscritos o la creación de nuevos ficheros con el fin de que la citada unidad de la Universidad pueda proceder a recabar los datos que necesita.

La Universidad declaró sus ficheros ante la Agencia Vasca de Protección de Datos en el año 2007. Cuando sea necesario recabar datos diferentes a los indicados en dichos ficheros, se procederá a su modificación o la creación de nuevos ficheros.

28.4. En el *Anexo I. M VIII* se adjuntan los ficheros declarados en virtud del Acuerdo adoptado por el Consejo de Gobierno de la UPV/EHU de 8 de febrero de 2007 para la creación, modificación y supresión de ficheros de datos de carácter personal de la Universidad, publicado por Resolución de 28 de febrero de 2007 del Secretario General de la UPV/EHU (BOPV n.º 69, de 11 de abril de 2007).

TÍTULO IV.
RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS

Artículo 29
Responsable de Seguridad LOPD

29.1. La UPV/EHU tendrá una persona responsable de seguridad de carácter general para toda la Universidad, en adelante Responsable de Seguridad LOPD, el cual será la persona encargada de definir y velar por el cumplimiento de la estrategia global en materia de seguridad de la información de la UPV/EHU, y especialmente, la correcta adecuación de la misma a lo establecido en la normativa relativa a la protección de datos de carácter personal.

El «Responsable de Seguridad LOPD» es la persona de contacto para cualquier cuestión relacionada con la protección de datos de carácter personal.

29.2. Las funciones de la persona Responsable de Seguridad LOPD serán, entre otras, las siguientes:

a) encargarse de canalizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, las revocaciones de consentimiento y las impugnaciones de valoraciones que puedan presentarse;

b) supervisar las solicitudes de cesión de datos a entidades externas;

c) resolver cuantas dudas puedan suscitarse en relación con la protección de datos de carácter personal;

d) redactar y controlar las cláusulas informativas y documentos de autorización en relación con la protección de datos de carácter personal;

e) resto de funciones que puedan ser encomendadas por este Reglamento o las competentes instancias universitarias.

Artículo 30
Máximo Responsable de los ficheros y Responsables Internos de fichero

30.1. El Rector o Rectora será la máxima persona responsable de la efectiva aplicación de la normativa en materia de protección de datos de carácter personal por parte de la UPV/EHU, y responsable último de todos los ficheros declarados por la UPV/EHU.

No obstante, cada fichero tendrá una persona Responsable Interno de fichero, que por delegación del Rector o Rectora, decidirá sobre la finalidad, contenido y tratamiento del fichero que se le asigne. La persona Responsable Interno del fichero cumplirá las funciones asignadas por la ley o este Reglamento a la persona Responsable del fichero o tratamiento en relación al fichero que le ha sido adjudicado.

El Rector o Rectora es la persona responsable última de todos los ficheros declarados por la UPV/EHU.
No obstante, las personas nombradas «Responsables Internos de fichero» responderán de la finalidad, contenido y tratamiento de los ficheros que se les asignen.

30.2. La persona Responsable Interno del fichero será la encargada de:

a) la seguridad del fichero, por lo que se responsabilizará de la implantación de la normativa universitaria relacionada con la seguridad informática y la protección de datos en relación con el fichero que le ha sido asignado;
b) llevar a cabo las acciones necesarias para que el personal de la UPV/EHU, especialmente los Coordinadores o Coordinadoras de la protección de datos de carácter personal de Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u organismo universitario, conozcan las normas que afectan al desarrollo de sus funciones en relación con su fichero, así como las consecuencias en que pudieran incurrir en caso de incumplimiento;
c) resto de funciones que puedan ser encomendadas por este Reglamento o las competentes instancias universitarias.

30.3. Una misma persona podrá ser Responsable Interno de varios ficheros.

Artículo 31
Comité de Seguridad Informática y Gestión Documental

31.1. Los Responsables Internos de los ficheros designarán a un comité, el «**Comité de Seguridad Informática y Gestión Documental**», como «Responsable de Seguridad» (según definición del RDLOPD) de sus ficheros. Por lo tanto, dicho comité será el encargado de coordinar y controlar las medidas de seguridad aplicables en relación con todos los ficheros de la UPV/EHU y para ello, podrá apoyarse en las personas que estime oportuno.

El «Comité de Seguridad Informática y Gestión Documental» se ocupa de coordinar y controlar las medidas de seguridad aplicables a los ficheros.

31.2. La composición de este Comité será la siguiente:

— El Vicegerente o Vicegerenta de Tecnologías de la Información y las Comunicaciones (o Vicegerente designado por el Gerente).
— La persona Responsable de Seguridad LOPD.
— Una persona de cada Centro de Informática de la Universidad.
— El o la técnico de Archivo de Secretaría General.
— Una persona del Servicio Jurídico.

Artículo 32
Comisión para la Protección de Datos

32.1. Esta Comisión se reunirá al menos semestralmente con el objeto de llevar a cabo el control y la coordinación de la efectiva implantación del presente Reglamento y establecer las pautas de actuación de la UPV/EHU en cuestión de protección de datos.

32.2. La composición de esta Comisión será la siguiente:

— El Vicegerente o Vicegerenta de Recursos Generales (o Vicegerente designado por el Gerente).
— La persona Responsable de Seguridad LOPD.
— Dos personas Responsables Internos de Fichero designados por el Rector o Rectora a propuesta de la persona Responsable de Seguridad LOPD.

La «Comisión para la Protección de Datos» controla y coordina la implantación de la normativa en materia de protección de datos.

— El Jefe o Jefa de Secretaría General.
— Una persona del Servicio Jurídico.
— Un Administrador o Administradora de Centro universitario designado por el Gerente o Gerenta.
— Un Secretario o Secretaria de Campus designado por el Rector o Rectora a propuesta del Secretario o Secretaria General.

32.3. Las funciones de la Comisión para la Protección de Datos, entre otras, serán las siguientes:

a) supervisar la implantación del presente Reglamento y promover medidas para la consecución de su efectiva aplicación;
b) proponer e impulsar la aprobación de las actualizaciones necesarias del presente Reglamento ante los órganos universitarios competentes;
c) realizar un seguimiento de los derechos de acceso, rectificación, cancelación y oposición, revocación del consentimiento e impugnación de valoraciones que se presenten ante la persona Responsable de Seguridad LOPD;
d) resto de funciones que puedan ser encomendadas por este Reglamento o las competentes instancias universitarias.

Artículo 33
Coordinador o Coordinadora de la protección de datos de carácter personal de Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u otro organismo universitario

El máximo o máxima responsable del Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u otro organismo universitario será la persona encargada de difundir, implantar y garantizar la efectiva aplicación de la normativa relativa a la protección de datos de carácter personal de la Universidad en el ámbito que le corresponda, en coordinación y colaboración con el resto de responsables en materia de protección de datos de carácter personal de la Universidad, y pudiendo designar a su vez a otras personas para estar tareas sin que ello implique una delegación de su responsabilidad.

La persona responsable del Rectorado y cada Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u organismo universitario, se ha de encargar en su ámbito de: difundir, implantar y garantizar la aplicación de la normativa de protección de datos de carácter personal.

TÍTULO V.
MEDIDAS DE SEGURIDAD

CAPÍTULO 1

Medidas de aplicación general

Artículo 34
Niveles de seguridad

34.1. Se establecen tres niveles de seguridad —básico, medio y alto—, que deben aplicarse a los ficheros y tratamientos, tanto automatizados como no automatizados, atendiendo a la naturaleza de la información tratada y en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

En función de la naturaleza de la información y la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información, se establecen tres niveles de seguridad: básico, medio y alto.

34.2. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

34.3. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de carácter personal:

— Los relativos a la comisión de infracciones administrativas o penales.
— Aquellos de los que sean responsables las Administraciones Tributarias, las entidades financieras, las entidades dedicadas la prestación de servicios de información sobre solvencia patrimonial y crédito, las Entidades Gestoras y Servicios Comunes de la Seguridad Social, y las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

— Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de las ciudadanas o ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

34.4. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

— Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
— Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
— Aquéllos que contengan datos derivados de actos de violencia de género.

34.5. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 del RDLOPD.

34.6. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que las afectadas o afectados sean asociados o miembros.
b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

34.7. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado o afectada, con motivo del cumplimiento de deberes públicos.

34.8. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplica-

ción en cada caso o las que por propia iniciativa adoptase la persona Responsable del fichero o tratamiento.

La UPV/EHU garantiza que, como mínimo, adoptará las medidas recogidas en las disposiciones legales o reglamentarias para cada nivel de seguridad.

34.9. A los efectos de facilitar el cumplimiento de lo dispuesto en este Título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios o usuarias con acceso a los mismos, y que esto se haga constar en el Documento de Seguridad.

34.10. En el *Anexo I. M IX* y *Anexo I. M X* se incluye un cuadro resumen sobre las medidas de seguridad aplicables a los ficheros automatizados y no automatizados, respectivamente, en función de lo establecido por el RDLOPD.

Artículo 35
Encargado del tratamiento

35.1. Cuando la persona Responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un Encargado del tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el Documento de Seguridad de dicha persona Responsable, comprometiéndose el personal del Encargado del tratamiento al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al Encargado del tratamiento incorporar tales datos a sistemas o soportes distintos de los de la persona Responsable, este último deberá hacer constar esta circunstancia en el Documento de Seguridad de la persona Responsable, comprometiéndose el personal del Encargado del tratamiento al cumplimiento de las medidas de seguridad previstas en el citado documento.

35.2. Si el servicio fuera prestado por el Encargado del tratamiento en sus propios locales, ajenos a los de la persona Responsable del fichero o tratamiento, deberá elaborar un Documento de Seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y la persona Responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

35.3. En todo caso, el acceso a los datos por el Encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este Reglamento.

El personal que trabaja para el «Encargado del tratamiento» tiene que cumplir las medidas recogidas en el presente Reglamento.

Artículo 36
Prestaciones de servicios sin acceso a datos de carácter personal

La persona Responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos de carácter personal, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos de carácter personal.

El personal de la UPV/EHU debe tener acceso sólo a aquellos datos de carácter personal que sean estrictamente necesarios para la realización de las funciones que tiene encomendadas.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos de carácter personal y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 37
Delegación de autorizaciones

Las autorizaciones que en este Título se atribuyen la persona Responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el Documento de Seguridad deberán constar las personas habili-

tadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde a la persona Responsable del fichero o tratamiento.

Artículo 38
Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 34 del presente Reglamento.

Artículo 39
Régimen de trabajo fuera de los locales de la persona Responsable del fichero o tratamiento o Encargado o Encargada del tratamiento

39.1. Cuando los datos de carácter personal se almacenen en dispositivos portátiles o se traten fuera de los locales de la persona Responsable de fichero o tratamiento, o del Encargado o Encargada del tratamiento será preciso que exista una autorización previa de la persona Responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Sólo podrán incorporarse datos de carácter personal a dispositivos portátiles previa autorización de la persona «Responsable del fichero o tratamiento».

39.2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el Documento de Seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 40
Ficheros temporales o copias de trabajo de documentos

40.1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxi-

liares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 34 del presente Reglamento.

40.2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Los ficheros temporales serán borrados o destruidos cuando dejen de ser necesarios.

CAPÍTULO 2

Documento de Seguridad y Auditoría

Artículo 41
Documento de Seguridad

41.1. La UPV/EHU implantará la normativa de seguridad mediante un documento que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente. Dicho documento será de obligado cumplimiento para el personal con acceso a datos de carácter personal y sistemas de información.

41.2. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

El «Documento de Seguridad» recoge las medidas de índole técnica y organizativa, y es de cumplimiento obligatorio.

g) Las medidas que sea necesario adoptar para el transporte de documentos y soportes, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

h) Las medidas de seguridad adoptadas respecto de los ficheros o tratamientos no automatizados.

i) La identificación de la persona «responsable de seguridad», es decir, el Comité de Seguridad Informática y Gestión Documental.

j) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

41.3. Cuando exista un tratamiento de datos por cuenta de terceros, el Documento de Seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de Encargado o Encargada con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

41.4. En aquellos casos en los que datos de carácter personal de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del Encargado, la persona Responsable del fichero o tratamiento deberá anotarlo en el Documento de Seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos de la persona Responsable del fichero o tratamiento, podrá delegarse en el Encargado del tratamiento la llevanza del Documento de Seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre de protección de los datos de carácter personal, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al Documento de Seguridad del Encargado al efecto del cumplimiento de lo dispuesto por este Reglamento.

41.5. El Documento de Seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

41.6. El contenido del Documento de Seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El «Documento de Seguridad» será actualizado con el fin de que sea fiel reflejo de los sistemas de información de la Universidad y las disposiciones vigentes en materia de seguridad.

Artículo 42
Auditoría

42.1. A partir del nivel medio de medidas de seguridad, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento del presente Título. Con carácter extraordinario deberá realizarse dicha auditoria siempre que se realicen modificaciones en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoria inicia el cómputo de dos años señalado en el párrafo anterior.

Al menos cada dos años se llevará a cabo una auditoria que verifique el grado de cumplimiento de las medidas de seguridad a respetar.

42.2. El informe de auditoria deberá dictaminar sobre la adecuación de las medidas y controles tanto al presente Reglamento como a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

42.3. Los informes de auditoria serán analizados por la persona Responsable de Seguridad LOPD, que elevará las conclusiones a los Responsables Internos de los Ficheros, al Comité de Seguridad Informática y Gestión Documental, y a la Comisión para la Protección de Datos, con el fin de que adopten las medidas correctoras adecuadas. Asimismo, quedarán a disposición de la Agencia Vasca de Protección de Datos.

CAPÍTULO 3

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección primera
MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 43
Funciones y obligaciones del personal

43.1. Las funciones y obligaciones de cada uno de los usuarios y usuarias o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el Documento de Seguridad.
También se definirán las funciones de control o autorizaciones delegadas por la persona Responsable del fichero o tratamiento.

La persona «Responsable de fichero o tratamiento» se encargará de que las personas que realizan tratamientos de datos de carácter personal conozcan y respeten las medidas de seguridad.

43.2. La persona Responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 44
Registro de incidencias

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Se ha de reflejar en el Registro de incidencias cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Artículo 45
Control de acceso

45.1. Las usuarias o usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

45.2. La persona Responsable del fichero o tratamiento se encargará de que exista una relación actualizada de usuarias o usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

45.3. La persona Responsable del fichero o tratamiento establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

45.4. Exclusivamente el personal autorizado para ello en el Documento de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por la persona Responsable del fichero o tratamiento.

Solamente las personas indicadas en el «Documento de Seguridad» tienen capacidad para conceder autorizaciones para el acceso a recursos que contienen datos de carácter personal.

45.5. En caso de que exista personal ajeno a la persona Responsable del fichero o tratamiento que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 46
Gestión de soportes y documentos

46.1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el Documento de Seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Documento de Seguridad.

46.2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control de la persona Responsable del fichero o tratamiento deberá ser autorizada por la persona Responsable del fichero o tratamiento encontrarse debidamente autorizada en el Documento de Seguridad.

46.3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Las salidas y traslados de soportes y documentos que contengan datos de carácter personal deben ser previamente autorizados y llevarse a cabo con las medidas de seguridad pertinentes.

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

Artículo 47
Identificación y autenticación

47.1. La persona Responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. Para ello podrán utilizarse entre otros, mecanismos basados en certificados digitales electrónicos o en el reconocimiento de datos biométricos.

47.2. La persona Responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario o usuaria que intente acceder al sistema de información y la verificación de que está autorizado.

47.3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Como mínimo una vez al año, se procederá al cambio de las contraseñas.

47.4. El Documento de Seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 48
Copias de respaldo y recuperación

48.1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

48.2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el Documento de Seguridad.

48.3. La persona Responsable del fichero o tratamiento se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Al menos semanalmente, se realizarán copias de respaldo.

48.4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el Documento de Seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Sección segunda
MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 49
Auditoría

49.1. A partir del nivel medio la auditoria, al menos cada dos años, de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos será obligatoria.

Artículo 50
Gestión de soportes y documentos

50.1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

En relación con los datos que requieran medidas de seguridad de nivel medio, se establecerán sistemas de control en la entrada y salida de los soportes.

50.2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, la persona destinataria, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 51
Identificación y autenticación

La persona Responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Se limitará el intentar acceder de forma reiterada y fallida a los sistemas de información.

Artículo 52
Control de acceso físico

Exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 53
Registro de incidencias

53.1. En el registro regulado en el artículo 44 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

53.2. Será necesaria la autorización de la persona Responsable del fichero o tratamiento para la ejecución de los procedimientos de recuperación de los datos.

Sección tercera
MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 54
Gestión y distribución de soportes

54.1. La identificación de los soportes o documentos se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios o usuarias con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

54.2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control de la persona Responsable del fichero o tratamiento.

54.3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el Documento de Seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 55
Copias de respaldo y recuperación

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este Título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

En relación con los datos que requieran medidas de seguridad de nivel alto, deberá conservarse una copia de respaldo en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan.

Artículo 56
Registro de accesos

56.1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario o usuaria, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

56.2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

56.3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del «responsable de seguridad» competente, es decir, el Comité de Seguridad Informática y Gestión Documental, sin que deban permitir la desactivación ni la manipulación de los mismos.

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

56.5. La persona Responsable de Seguridad LOPD, junto con el Comité de Seguridad Informática y Gestión Documental, se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

56.6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que la persona Responsable del fichero o del tratamiento sea una persona física.
b) Que la persona Responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos de carácter personal.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el Documento de Seguridad.

Artículo 57
Telecomunicaciones

La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO 4

Medidas de seguridad aplicables a ficheros y tratamientos no automatizados

Sección primera
MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 58
Obligaciones comunes

58.1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los Capítulos I y II del presente Título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado o encargada del tratamiento.
d) Prestaciones de servicios sin acceso a datos de carácter personal.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales de la persona Responsable del fichero o tratamiento o Encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de Seguridad.

58.2. Asimismo se les aplicará lo establecido por la Sección Primera del Capítulo III del presente Título en lo relativo a:

a) Funciones y obligaciones del personal.
b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 59
Criterios de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en la respectiva normativa universitaria aplicable. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

La «Comisión de Valoración y Expurgo o Comisión de Archivo» de la Universidad se encarga de fijar los criterios de archivo (BOPV nº 170, de 7 septiembre de 2005).

En aquellos casos en los que no exista norma aplicable, la persona Responsable del fichero o tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 60
Dispositivos de almacenamiento

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, la persona Responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Todos los armarios y demás dispositivos de almacenamiento deben disponer de mecanismos que dificulten su apertura.

Artículo 61
Custodia de los soportes

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección segunda
MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 62
Auditoría

A partir del nivel medio la auditoria interna o externa de los ficheros, al menos cada dos años, será obligatoria.

Sección tercera
MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 63
Almacenamiento de la información

63.1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal de nivel alto deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

63.2. Si, atendidas las características de los locales de que dispusiera la persona Responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, la persona responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el Documento de Seguridad.

Deben permanecer cerrados los lugares en los que se almacenen soportes con datos de seguridad de nivel alto en ficheros no automatizados (por ejemplo, en papel). En el caso de traslado de documentación, se adoptarán medidas para impedir el acceso o manipulación de la información.

Artículo 64
Copia o reproducción

64.1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el Documento de Seguridad.

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

Artículo 65
Acceso a la documentación

65.1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

65.2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos, que puedan ser utilizados por múltiples usuarios o usuarias.

65.3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el Documento de Seguridad.

Artículo 66
Traslado de documentación

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

TÍTULO VI.
LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

Artículo 67
La Agencia Vasca de Protección de Datos

67.1. La Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, configura a ésta como ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones.

67.2. La Agencia Vasca de Protección de Datos asume como misión proteger la intimidad personal y familiar de los ciudadanos o ciudadanas y el legítimo ejercicio de sus derechos, velando por el cumplimiento de la normativa sobre protección de datos de carácter personal. En el ejercicio de su actividad, tiene la consideración de autoridad de control y la ley le garantiza la plena independencia y objetividad en el ejercicio de su cometido.

La Agencia Vasca de Protección de Datos controla la actuación de la UPV/EHU en materia de protección de datos, actuando con plena independencia en el ejercicio de sus funciones.

67.3. Entre las entidades públicas que están dentro del ámbito de control de la Agencia Vasca de Protección de Datos se encuentra la UPV/EHU.

Artículo 68
Actividades de la Agencia Vasca de Protección de Datos

Para el ejercicio de las funciones que la ley confiere a la Agencia Vasca de Protección de Datos, ésta desempeña, entre otras, las siguientes tareas o actividades:

a) Informar a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal y ayudarles y tutelarles en el ejercicio de los mismos.
b) Investigar aquellas actuaciones contrarias a la ley y resolver, en su caso, sobre las infracciones producidas y requerir la adopción de las medidas necesarias para la adecuación del tratamiento de datos a la legislación en vigor.
c) Mantener un Registro de Ficheros de Datos de Carácter Personal, en el cual las administraciones públicas y entes de derecho público de la Comunidad Autónoma del País Vasco han de inscribir sus ficheros, declarando los tipos de datos de carácter personal que recogen y tratan para el cumplimiento de sus fines.
d) Atender todo tipo de consultas e informes que, en relación a la protección de datos, le sean solicitados por personas e instituciones.
e) Difundir y extender la cultura de la protección de datos, sensibilizando a los colectivos sociales y potenciando la formación y la adopción de mejores prácticas por parte de los trabajadores de las instituciones públicas.

DISPOSICIÓN TRANSITORIA

El carácter vinculante para la UPV/EHU de las medidas de seguridad previstas en el Título V del presente Reglamento, se ajustará a lo establecido en la Disposición Transitoria Segunda del RDLOPD en relación con la obligatoriedad de las medidas de seguridad exigidas por dicho RDLOPD.

DISPOSICIÓN FINAL

ACTUALIZACIÓN DEL REGLAMENTO Y DE LOS ANEXOS-ENTRADA EN VIGOR

Este Reglamento será periódicamente actualizado en función de los nuevos requisitos normativos que puedan ser exigidos y los supuestos susceptibles de regulación que se vayan detectando.

Las modificaciones e incorporaciones de Anexos podrán ser realizadas mediante acuerdo adoptado por la mayoría de los miembros del Consejo de Dirección de la UPV/EHU, a propuesta conjunta de la Secretaría General y la Gerencia.

Este Reglamento es de obligado cumplimiento desde el curso académico 2008-2009.

La Comisión para la Protección de Datos podrá enviar a la Secretaría General sus propuestas de cambio.

La versión actualizada del Reglamento estará disponible en la página web de la Universidad (*www.ehu.es/babestu*).

El presente Reglamento entrará en vigor el 1 de octubre de 2008, una vez de haber sido debidamente registrado en la Agencia Vasca de Protección de Datos.

ANEXO I.
MODELOS E INFORMACIÓN COMPLEMENTARIA

M I. Cláusula informativa tipo en documentos y/o pantallas.

De acuerdo con lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que sus datos pasan a formar parte del fichero _____ de la UPV/EHU, cuya finalidad es _____.

Le comunicamos que puede ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos remitiendo un escrito a la persona Responsable de Seguridad LOPD de la UPV/EHU, Rectorado, Barrio Sarriena s/n, 48940 Leioa-Bizkaia, adjuntando copia de documento que acredite su identidad.

Puede consultar el «Reglamento de la UPV/EHU para la Protección de Datos de carácter Personal» en las direcciones de Internet *www.ehu.es/babestu*.

M II. Revocación del consentimiento para el tratamiento de datos

Solicitud de revocación de consentimiento otorgado para el tratamiento de mis datos de carácter personal por parte de la UPV/EHU

Datos del fichero/s en el/los que solicito la revocación de mi consentimiento al tratamiento de mis datos de carácter personal

Nombre del fichero/s						
Descripción del tratamiento						
Fecha del Consentimiento						
Dirigido a	UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA Vicegerencia de las Tecnologías de la Información y las Comunicaciones A la atención de: **Responsable de Seguridad LOPD**					
Barrio	Sarriena		N.º	—	Piso	—
Localidad	Leioa	Terr. Histórico	Bizkaia		Cód. postal	48940

Datos del o de la solicitante

Apellidos					
Nombre		D.N.I.			
Calle			N.º	Piso	
Localidad		Terr. Histórico		Cód. postal	
Telefono		Correo electrónico			

Datos del o de la representante legal

Apellidos			
Nombre		D.N.I.	

SOLICITO:

1) **La revocación del consentimiento** dado para el tratamiento arriba descrito por parte de la UPV/EHU.
2) **Notificarme** la materialización de la revocación de consentimiento planteada.
3) **Notificar** a las personas responsables de ficheros o tratamientos a quiénes hubieran sido comunicados los datos la revocación del consentimiento practicada.

Lugar y fecha	
Firma del o de la solicitante	

INFORMACIÓN COMPLEMENTARIA

I. Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito

— Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.
— En todo caso, será necesario la entrega de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho del interesado.
— En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del **documento acreditativo auténtico** de la representación legal.

II. Requisitos del procedimiento para el que ejercita el derecho

— La revocación del consentimiento se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de

la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149 de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

— Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III. Requisitos del procedimiento para la persona Responsable del Fichero o tratamiento

— La persona responsable deberá responder al o a la solicitante en el **plazo máximo de diez días hábiles**, a contar desde la recepción de la solicitud.
— Transcurrido este plazo sin que de forma expresa se conteste a la petición de acceso, ésta se entenderá denegada.
— **Si la solicitud de revocación del consentimiento fuese estimada, la persona responsable deberá informar** a la persona interesada, en la forma elegida por éste, **en el plazo de diez días hábiles** a contar desde la fecha de la recepción de la solicitud.
— A la revocación del consentimiento no se le atribuirán efectos retroactivos.
— La materialización de la revocación del consentimiento al tratamiento de datos es **gratuita**.

IV. Normativa de aplicación

— Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículo 6.3.
— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículo 17.
— Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículo 11.5.

V. Reclamaciones (Tutela de derechos)

— Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de revocación del consentimiento otorgado para el tratamiento de sus propios datos, puede reclamar ante la **Agencia Vasca de Protección de Datos** para que inicie un procedimiento de tutela de sus derechos.

— Para ello, resulta necesario que haya transcurrido el plazo de diez días desde la solicitud del derecho de revocación del consentimiento para el tratamiento de sus propios datos, sin que de forma expresa se le haya contestado.
— La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (C/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 016 230- Fax. 945 016 231 *avpd@avpd.es - www.avpd.es*), aportándose alguno de los siguientes documentos:

- La negativa de la persona Responsable de Seguridad LOPD a llevar a cabo la revocación del consentimiento.
- Copia del modelo de revocación del consentimiento, sellada por el registro de entrada de la UPV/EHU.
- Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

M III. Consentimiento para el tratamiento de datos

DATOS DE LA PERSONA INTERESADA

D./D.ª ....., mayor de edad, con domicilio en la c/ ....., n.º ....., Localidad ....., Provincia ..... Código Postal ..... con D.N.I. ....., del que se acompaña fotocopia, por medio del presente escrito manifiesta que:

> Por la presente autoriza el tratamiento de sus datos de carácter personal y su inclusión en el fichero de [introducir fichero correspondiente] de la UPV/EHU, cuya finalidad es [introducir la finalidad del fichero correspondiente], de acuerdo con lo dispuesto en la Declaración de ficheros de la UPV/EHU publicada de el BOPV n.º 69, de 11 de abril de 2007.

De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y en función de lo establecido en el Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de fecha 10 de abril de 2008, la persona interesada tendrá la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, mediante escrito dirigido a la persona Responsable de Seguridad LOPD de la UPV/EHU, Rectorado, Barrio Sarriena s/n, 48940 Leioa-Bizkaia, adjuntando copia de documento que acredite su identidad.

Firma de la persona interesada:

ADVERTENCIA:

* En el caso de que se recabasen datos relativos a la ideología, religión o creencias de la persona interesada, éste deberá ser advertido de su derecho a no consentir el tratamiento de tales datos.

M IV. Derecho de acceso

Solicitud de ejercicio del derecho de acceso a mis datos de carácter personal inscritos en fichero de la UPV/EHU

Datos del fichero/s en el/los que solicito el acceso a mis datos de carácter personal

Nombre del fichero/s						
Dirigido a	UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA Vicegerencia de las Tecnologías de la Información y las Comunicaciones A la atención de: **Responsable de Seguridad LOPD**					
Barrio	Sarriena		N.º	—	Piso	—
Localidad	Leioa	Terr. Histórico	Bizkaia		Cód. postal	48940

Datos del o de la solicitante

Apellidos					
Nombre		D.N.I.			
Calle			N.º	Piso	
Localidad		Terr. Histórico		Cód. Postal	
Telefono		Correo electrónico			

Datos del o de la representante legal

Apellidos			
Nombre		D.N.I.	

Deseo ejercer mi derecho de acceso, de conformidad con lo establecido en la normativa sobre protección de datos, por lo que **SOLICITO se me facilite gratuitamente el derecho de acceso a el/los fichero/s indicado/s**, informándome sobre todos mis datos de carácter personal en él/ellos contenidos, en el plazo máximo de un mes a contar desde la recepción de esta solicitud. Deseo que la in-

formación solicitada me sea facilitada, siempre que sea materialmente posible de la siguiente manera:

- ☐ Presencialmente mediante visualización en pantalla.
- ☐ Escrito, copia o fotocopia remitida por correo a la dirección indicada.
- ☐ Correo electrónico u otros sistemas de comunicaciones electrónicas.
- ☐ Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero o la naturaleza del tratamiento.

Lugar y fecha	
Firma del o de la solicitante	

INFORMACIÓN COMPLEMENTARIA

I. Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito

— Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.
— En todo caso, será necesario la entrega de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho de la persona interesada.
— En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del **documento acreditativo auténtico** de la representación legal.

II. Requisitos del procedimiento para el que ejercita el derecho

— El derecho de acceso **no podrá llevarse a cabo en intervalos inferiores a 12 meses**, salvo interés legítimo debidamente justificado.
— El derecho de acceso se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

— Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III. Requisitos del procedimiento para la persona Responsable del Fichero o tratamiento

— La persona responsable deberá responder al o a la solicitante en el **plazo máximo de un mes**, a contar desde la recepción de la solicitud.
— Transcurrido este plazo sin que de forma expresa se conteste a la petición de acceso, ésta se entenderá denegada.
— **Si la solicitud del derecho de acceso fuese estimada, la persona responsable deberá informar** a la persona interesada, en la forma elegida por éste, **en el plazo de diez días hábiles** a contar desde la fecha de la estimación. Al margen de la opción de consulta seleccionada por la persona interesada, la UPV/EHU podrá determinar el sistema de consulta cuando el requerido por la persona interesada perturbe la normal prestación de los servicios de la Universidad.
— La información deberá contener de modo legible e inteligible los datos incluidos en el fichero y los resultantes de cualquier elaboración, proceso o tratamiento, así como el **origen de los datos, los cesionarios** (instituciones y organizaciones públicas o privadas a los que se ha comunicado o se prevé comunicar tales datos) **y la especificación de los usos concretos y finalidades** para los que se almacenaron.
— La entrega de datos es **gratuita**.

IV. Normativa de aplicación

— Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículo 15.
— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículos 23, 24, 25, 26, 27, 28, 29 y 30.
— Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de creación de la Agencia Vasca de Protección de Datos, artículo 8 y 9.
— Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, artículos 6, 7 y 8.
— Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículos 13, 14 y 18.

V. Reclamaciones (Tutela de derechos)

— Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de acceso a sus propios datos, puede reclamar ante la **Agencia Vasca de Protección de Datos** para que inicie un procedimiento de tutela de sus derechos.
— Para ello, resulta necesario que haya transcurrido el plazo de un mes desde la solicitud del derecho de acceso, sin que de forma expresa se le haya contestado.
— La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (C/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 016 230- Fax. 945 016 231 *avpd@avpd.es - www.avpd.es*), aportándose alguno de los siguientes documentos:

- La negativa de la persona Responsable de Seguridad LOPD a facilitar la información solicitada.
- Copia del modelo de petición de acceso, sellada por el registro de entrada de la UPV/EHU.
- Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

M V. Derecho de rectificación

Solicitud de ejercicio del derecho de rectificación en mis datos de carácter personal inscritos en fichero de la UPV/EHU

Datos del fichero/s en el/los que solicito la rectificación de mis datos de carácter personal

Nombre del Fichero/s						
Dirigido a	UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA Vicegerencia de las Tecnologías de la Información y las Comunicaciones A la atención de: **Responsable de Seguridad LOPD**					
Barrio	Sarriena			N.º	—	Piso —
Localidad	Leioa	Terr. Histórico	Bizkaia		Cód. Postal	48940

Datos del o de la solicitante

Apellidos					
Nombre		D.N.I.			
Calle			N.º		Piso
Localidad		Terr. Histórico		Cód. Postal	
Telefono		Correo electrónico			

Datos del o de la representante legal

Apellidos			
Nombre		D.N.I.	

Deseo ejercer mi derecho de rectificación, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal, por lo que **SOLICITO se proceda a:**

1) **La rectificación de los siguientes datos erróneos relativos a mi persona** que se encuentran en el/los fichero/s referidos:

Dato erróneo	Dato correcto

O los datos que señalo en la hoja anexa

2) **Notificarme** la rectificación planteada.
3) **Notificar** a las personas responsables de los ficheros o tratamientos a quiénes hubieran sido comunicados los datos la rectificación practicada.

Lugar y fecha	
Firma del o de la solicitante	

INFORMACIÓN COMPLEMENTARIA

I. Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito

— Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.
— Se deberán entregar los documentos que se acompañen a la solicitud y que acrediten, en caso de ser necesario, la veracidad de los nuevos datos.
— En todo caso, será necesario la entrega de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho de la persona interesada.
— En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del **documento acreditativo auténtico** de la representación legal.

II. Requisitos del procedimiento para el que ejercita el derecho

— El derecho de rectificación se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
— Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III. Requisitos del procedimiento para la persona Responsable del fichero o tratamiento

— La persona responsable deberá responder al o a la solicitante en el **plazo máximo de diez días hábiles**, a contar desde la fecha de recepción de la solicitud.
— Transcurrido este plazo sin que de forma expresa se conteste a la petición de rectificación, ésta se entenderá denegada.
— Si la solicitud del derecho de rectificación fuese estimada, la persona responsable **deberá rectificar en el plazo de diez días hábiles** a contar desde la fecha de recepción de la solicitud.
— La rectificación de datos es **gratuita**.

IV. Normativa de aplicación

— Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículo 16.
— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículos 23, 24, 25, 26, 31, 32 y 33.
— Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de creación de la Agencia Vasca de Protección de Datos, artículo 8 y 9.
— Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, artículo 9.
— Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículos 13, 15 y 18.

V. Reclamaciones (Tutela de derechos)

— Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de rectificación de sus propios datos, puede reclamar ante la Agencia Vasca de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.
— Para ello, resulta necesario que haya transcurrido el plazo de diez días desde la solicitud del derecho de rectificación, sin que de forma expresa se le haya contestado.
— La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (C/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 016 230- Fax. 945 016 231 *avpd@avpd.es - www.avpd.es*), aportándose alguno de los siguientes documentos:

- La negativa de la persona Responsable del fichero o tratamiento a la rectificación solicitada.
- Copia del modelo de petición de rectificación, sellada por el registro de entrada de la UPV/EHU.
- Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

M VI. Derecho de cancelación

Solicitud de ejercicio del derecho de cancelación de mis datos de carácter personal inscritos en fichero de la UPV/EHU

Datos del fichero/s en el/los que solicito la cancelación de mis datos de carácter personal

Nombre del Fichero/s						
Dirigido a	UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA Vicegerencia de las Tecnologías de la Información y las Comunicaciones A la atención de: **Responsable de Seguridad LOPD**					
Barrio	Sarriena		N.º	—	Piso	—
Localidad	Leioa	Terr. Histórico	Bizkaia		Cód. Postal	48940

Datos del o de la solicitante

Apellidos					
Nombre		D.N.I.			
Calle			N.º	Piso	
Localidad		Terr. Histórico		Cód. Postal	
Telefono		Correo electrónico			

Datos del o de la representante legal

Apellidos			
Nombre		D.N.I.	

Deseo ejercer mi derecho de cancelación, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal. Para ello:

☐ Adjunto documentación justificativa de la cancelación.

☐ Revoco el consentimiento otorgado anteriormente, y no adjunto ninguna documentación adicional.

Por lo que SOLICITO se proceda a:

1) **la cancelación de cualquier dato relativo a mi persona** que se encuentre en el/los fichero/s referidos, al no existir vinculación jurídica o disposición legal que justifique su mantenimiento.
2) **notificarme** la cancelación solicitada.
3) **notificar** a los responsables de ficheros o tratamientos a quiénes hubieran sido comunicados los datos la cancelación para que ellos también procedan a realizar las modificaciones oportunas.

Lugar y fecha	
Firma del o de la solicitante	

INFORMACIÓN COMPLEMENTARIA

I. Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito

— Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.
— **En necesario adjuntar documentación justificativa de la cancelación** o, en su caso, revocar el consentimiento otorgado anteriormente.
— En todo caso, será necesario la entrega de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho de la persona interesada.
— En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del **documento acreditativo auténtico** de la representación legal.

II. Requisitos del procedimiento para el que ejercita el derecho

— El derecho de cancelación se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

— Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III. Requisitos del procedimiento para la persona Responsable del fichero o tratamiento

— La persona responsable deberá responder al o a la solicitante en el **plazo máximo de diez días hábiles**, a contar desde la fecha de recepción de la solicitud.
— Transcurrido este plazo sin que de forma expresa se conteste a la petición de cancelación, ésta se entenderá denegada.
— Si la solicitud del derecho de cancelación fuese estimada, la persona responsable **deberá cancelar los datos en el plazo de diez días hábiles** a contar desde la fecha de recepción de la solicitud.
— La **cancelación** dará lugar al **bloqueo** de los datos conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse al **borrado definitivo** y se volverá a informar a la persona interesada de ello.
— En los casos en los que claramente no existan potenciales responsabilidades nacidas del tratamiento, se procederá al **borrado físico de los datos,** excepto cuando la misma no sea materialmente posible, en cuyo caso la persona responsable procederá al **bloqueo** de los datos con el fin de impedir su utilización y tratamiento.
— La cancelación de datos es **gratuita**.

IV. Normativa de aplicación

— Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículo 16.
— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículos 23, 24, 25, 26, 31, 32 y 33.
— Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de creación de la Agencia Vasca de Protección de Datos, artículos 8 y 9.
— Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, artículo 9.

— Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículos 13, 16 y 18.

V. Reclamaciones (Tutela de derechos)

— Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de cancelación de sus propios datos, puede reclamar ante la Agencia Vasca de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.
— Para ello, resulta necesario que haya transcurrido el plazo de diez días desde la solicitud del derecho de cancelación, sin que de forma expresa se le haya contestado.
— La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (C/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 016 230- Fax. 945 016 231 *avpd@avpd.es - www.avpd.es*), aportándose alguno de los siguientes documentos:

- La negativa de persona Responsable del fichero o tratamiento a la cancelación solicitada.
- Copia del modelo de petición de cancelación, sellada por el registro de entrada de la UPV/EHU.
- Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

M VII. Derecho de oposición

Solicitud de ejercicio del derecho de oposición a que se traten mis datos de carácter personal inscritos en fichero de la UPV/EHU

Datos del fichero/s en el/los que me opongo al tratamiento de mis datos de carácter personal

Nombre del Fichero/s						
Dirigido a	UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA Vicegerencia de las Tecnologías de la Información y las Comunicaciones A la atención de: **Responsable de Seguridad LOPD**					
Barrio	Sarriena			N.º	—	Piso —
Localidad	Leioa	Terr. Histórico	Bizkaia	Cód. Postal	48940	

Datos del o de la solicitante

Apellidos					
Nombre		D.N.I.			
Calle			N.º		Piso
Localidad		Terr. Histórico		Cód. Postal	
Telefono		Correo electrónico			

Datos del o de la representante legal

Apellidos			
Nombre		D.N.I.	

Deseo ejercer mi derecho de oposición al tratamiento de mis datos en los referidos ficheros, por existir motivos fundados y legítimos relativos a una concreta situación personal, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal y lo argumentado a continuación.

Mi argumentación

Descripción de los datos de carácter personal que se están tratando de manera inadecuada

Porqué es inadecuado el tratamiento

Documentación que acompaño para acreditar mi argumentación

Por lo que SOLICITO que se acceda a mi derecho de oposición en los términos anteriormente expuestos.

Lugar y fecha	
Firma del o de la solicitante	

INFORMACIÓN COMPLEMENTARIA

I. Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito

— Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.
— En el caso de que se trate **motivos fundados y legítimos relativos a una concreta situación personal** es necesaria la aportación de **copias de documentos que lo acrediten** a la persona Responsable del fichero o tratamiento.
— En todo caso, será necesario la entrega de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho de la persona interesada.

— En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la **fotocopia de DNI** o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del **documento acreditativo auténtico** de la representación legal.

II. Requisitos del procedimiento para el que ejercita el derecho

— El derecho de oposición se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
— Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III. Requisitos del procedimiento para la persona Responsable del fichero o tratamiento

— La persona responsable deberá responder al o a la solicitante en el **plazo máximo de diez días hábiles**, a contar desde la fecha de recepción de la solicitud.
— Transcurrido este plazo sin que de forma expresa se conteste a la petición de oposición, ésta se entenderá denegada.
— Si la solicitud del derecho de oposición fuese estimada, la persona responsable **deberá excluir el tratamiento o tratamientos a que se refiera en el plazo de diez días hábiles** a contar desde la fecha de recepción de la solicitud.
— La exclusión del tratamiento de datos es **gratuita**.

IV. Normativa de aplicación

— Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículos 6.4, y 17.
— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículos 23, 24, 25, 26, 34, 35 y 36.
— Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de creación de la Agencia Vasca de Protección de Datos, artículo 8 y 9.

— Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, artículo 5.
— Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículos 13, 17 y 18.

V. Reclamaciones (Tutela de derechos)

— Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de oposición de sus propios datos, puede reclamar ante la **Agencia Vasca de Protección de Datos** para que inicie un procedimiento de tutela de sus derechos.
— Para ello, resulta necesario que haya transcurrido el plazo de diez días desde la solicitud del derecho de oposición, sin que de forma expresa se le haya contestado.
— La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (C/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 016 230- Fax. 945 016 231 *avpd@avpd.es - www.avpd.es*), aportándose alguno de los siguientes documentos:

- La negativa de la persona Responsable del fichero o tratamiento a la exclusión del tratamiento solicitada.
- Copia del modelo de petición de oposición, sellada por el registro de entrada de la UPV/EHU.
- Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

M VIII. Ficheros de carácter personal declarados por la UPV/EHU

A continuación, se presentan los ficheros de carácter personal de la UPV/EHU inscritos en la Agencia Vasca de Protección de Datos en virtud del Acuerdo adoptado por el Consejo de Gobierno de la UPV/EHU de 8 de febrero de 2007 para la creación, modificación y supresión de ficheros de datos de carácter personal de la Universidad, publicado por Resolución de 28 de febrero de 2007 del Secretario General de la UPV/EHU (BOPV n.º 69 de 11 de abril de 2007).

1. **Acceso a la Universidad.** Gestión de los procesos de acceso a la Universidad.
2. **Matriculación en primer y segundo ciclo**. Gestión de los procesos de matriculación en primer y segundo ciclo de la Universidad.
3. **Matriculación en tercer ciclo**. Matriculación en masters y cursos de postgrado de la Universidad.
4. **Becas y Ayudas**. Datos de las personas que solicitan becas y ayudas de la Universidad.
5. **Expedición de títulos universitarios.** Gestión de los títulos universitarios.
6. **Enseñanzas Propias**. Gestión de la matrícula y de los expedientes del alumnado que cursa enseñanzas propias.
7. **Acceso a Tercer Ciclo**. Gestión de los procesos de acceso a los cursos de postgrado de la Universidad.
8. **Gestión de Doctorado**. Datos académicos y calificaciones del alumnado que lee su tesis doctoral en la Universidad.
9. **Expedientes Académicos**. Gestión de expedientes académicos.
10. **Nóminas**. Gestión de Nóminas y cotizaciones a la Seguridad Social.
11. **Fondo Social**. Gestión del Fondo Social para la prestación de ayudas para financiar gastos de carácter sanitario.
12. **Expediente de personal**. Gestión de recursos humanos. Gestión de los recursos humanos de la Universidad, Selección y administración de personal de la Universidad.
13. **Créditos de Consumo**. Fondo para la prestación de créditos al personal de la Universidad.
14. **Selección y provisión de puestos**. Bolsas de trabajo y convocatorias de acceso y provisión de puestos.
15. **Investigación nivel alto**. Fichero destinado a finalidades de investigación donde los datos de carácter personal necesarios se corresponden con el nivel alto.
16. **Gestión de la Investigación**. Gestión y tramitación de todas las subvenciones y ayudas de entidades públicas y privadas destinadas a actividades

de investigación, recopilando los estudios y análisis de la actividad investigadora desarrollada por los Departamentos y Centros de la Universidad.

17. **Investigación nivel medio**. Fichero destinado a finalidades de investigación donde los datos de carácter personal necesarios se corresponden con el nivel medio.
18. **Investigación nivel básico**. Fichero destinado a finalidades de investigación donde los datos de carácter personal necesarios se corresponden con el nivel básico.
19. P**rácticas en empresas y Bolsa de Empleo**. Fichero destinado a facilitar la realización de prácticas en empresas de alumnado de la UPV/EHU y búsqueda de empleo de alumnado egresado de la misma.
20. **Registro General.** Registro de entrada y salida de documentos.
21. **Secretaria General.** Registro de resoluciones, nombramientos, designaciones, pleitos judiciales y requerimientos de otras administraciones.
22. **Gestión de terceros**. Gestión financiera. Base de datos de gestión financiera, contabilidad presupuestaria y contabilidad financiera.
23. **Compras y contrataciones**. Proveedores y contratistas de la Universidad.
24. **Alumnado con necesidades educativas especiales**. Gestión de las adaptaciones necesarias para que el alumnado con necesidades educativas especiales pueda cursar sus estudios en la Universidad.
25. **Deportes y actividades culturales.** Gestión de actividades deportivas y eventos culturales.
26. **Prevención y asistencia médica**. Datos necesarios para el control sanitario, reconocimientos, seguimiento de consultas, prevención de riesgos.
27. **Registro de Pacientes de Clínica Odontológica**. Gestión administrativa y asistencial de la Clínica Odontológica de la UPV/EHU.
28. **Servicio Editorial.** Gestión de ventas, suscripciones y promoción editorial.
29. **Fichero auxiliar informático**. Fichero destinado a validar usuarios en sistemas y dominios, facilitar autenticación en diversas aplicaciones, y en general a cualquier tipo de gestión interna de recursos informáticos y de comunicaciones de la universidad.
30. **Biblioteca.** Gestión de préstamos y reservas de libros y revistas.
31. **Encuestas Calidad Docente**. Gestión de las encuestas de opinión y satisfacción sobre el profesorado, así como encuestas sobre aspectos generales relacionados con la docencia.
32. **Protocolo**. Envío de información, invitaciones a actos protocolarios de la UPV/EHU.
33. **Mecenazgo**. Soporte en los procesos de que un particular realice aportaciones voluntarias a la Universidad y de las certificaciones necesarias.

M IX. Resumen medidas de Seguridad RDLOPD (ficheros automatizados)

	Nivel básico: ficheros o tratamientos de datos de carácter personal	
	Nivel medio: ficheros o tratamientos de datos relativos a infracciones administrativas o penales, los que informen de servicios de solvencia patrimonial y crédito, los que sean de Administraciones tributarias, los de prestación de servicios financieros, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, los de las mutuas de accidentes de trabajo y los que permitan evaluar la personalidad	
	Nivel alto: ficheros o tratamientos de datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género	
Documento de seguridad	— Implanta la normativa de seguridad concretando el ámbito de aplicación del mismo, las medidas, normas, procedimientos y estándares de seguridad, las funciones y obligaciones del personal, la descripción de los ficheros y de los SSII y los procedimientos de gestión de incidencias, soportes y documentos y copias de seguridad — Establece las medidas a adoptar en caso de transporte, reutilización o desecho de soportes y documentos — Identifica al encargado del tratamiento y los ficheros afectados y esto se expresa en el DS y en el contrato — Se debe mantener actualizado tanto en lo relativo a la organización como a la legislación vigente	— Identifica al o los responsables de seguridad — Establece los controles periódicos de cumplimiento del documento
Responsable de seguridad		— Es el encargado de coordinar y controlar las medidas de seguridad del documento — Esto no supone exoneración de la responsabilidad del responsable del fichero

Auditoría		— Una interna o externa al menos cada 2 años o cuando se realicen cambios sustanciales en los SSII — Da lugar a un informe de auditoría sobre la adecuación a las medidas, las deficiencias identificadas y propone medidas correctoras — Es analizado por el responsable de seguridad — Queda a disposición de la AVPD	
Personal	— El Documento de Seguridad especifica las funciones y obligaciones de un modo claro y documentado — Se difunden entre el personal las normas que les afecten y las consecuencias por incumplimiento		
Identificación y autenticación	— Existen medidas para la identificación y autenticación de los usuarios — Se identifica unívoca y personalmente a cada usuario — Existe un procedimiento de gestión almacenamiento y distribución de contraseñas — Existe un procedimiento para controlar la caducidad de contraseñas y el almacenamiento ininteligible de las mismas	— Se establece un mecanismo que limite el número de intentos reiterados de acceso no autorizado	
Control y registro de accesos	— Cada usuario accede únicamente a los datos y recursos necesarios para el desarrollo de sus funciones — Existe una relación actualizada de usuarios, perfiles y accesos autorizados — Existen mecanismos para controlar los derechos con que se accede a los recursos — Existen mecanismos que gestionen la concesión de permisos de acceso sólo por personal autorizado en el Documento de Seguridad	— Se realiza un control de acceso físico a los locales donde se encuentren ubicados los sistemas de información	— Se registran los datos de cada intento de acceso. — Los datos se conservan 2 años — Está bajo control del responsable de seguridad — El responsable de seguridad realiza un informe mensual — Existe una excepción: persona física y acceso unipersonal

Gestión y distribución de soportes y documentos	— Se identifica el tipo de información que contienen. — Se mantiene un inventario — Se almacenan con acceso restringido — El responsable del fichero autoriza la salida de soportes — Se adoptan medidas en caso de desecho de soportes	— Existe un registro de entrada y salida de soportes que permite conocer el tipo de soporte o documento, la fecha y hora, el emisor o receptor, el tipo de información, la forma de envío y la persona responsable	— Existe un sistema de etiquetado solo comprensible para los usuarios autorizados — Se cifran los datos en la distribución de soportes y en los dispositivos portátiles
Copias de respaldo y recuperación	— Debe existir un procedimiento de copias de respaldo y recuperación de datos — El procedimiento garantiza la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción — Se realiza una copia de respaldo, al menos semanal — Verificación semestral de los procedimientos de copia por parte del responsable del fichero — Se trabaja sólo con datos reales si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado y se ha hecho una copia.		— Debe existir una copia de respaldo y de los procedimientos de recuperación en lugar diferente del que se encuentren los equipos
Registro de incidencias	— Se debe registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados	— Se debe registrar la realización de procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y grabados manualmente — El responsable del fichero autoriza la ejecución de los procedimientos de recuperación de datos	
Telecomunicaciones	— Las medidas de seguridad exigibles a los accesos a través de redes de comunicaciones deben garantizar un nivel de seguridad equivalente a los accesos en modo local		— La transmisión de datos a través de redes públicas o de redes inalámbricas debe ser cifrada

M X. Resumen medidas de Seguridad RDLOPD (ficheros no automatizados)

	Nivel básico: ficheros o tratamientos de datos de carácter personal
	Nivel medio: ficheros o tratamientos de datos relativos a infracciones administrativas o penales, los que informen de servicios de solvencia patrimonial y crédito, los que sean de Administraciones tributarias, los de prestación de servicios financieros, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, los de las mutuas de accidentes de trabajo y los que permitan evaluar la personalidad
	Nivel alto: ficheros o tratamientos de datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género
Documento de seguridad	— Implanta la normativa de seguridad concretando el ámbito de aplicación del mismo, las medidas, normas, procedimientos y estándares de seguridad, las funciones y obligaciones del personal, la descripción de los ficheros y de los SSII y los procedimientos de gestión de incidencias, soportes y documentos y copias de seguridad — Establece las medidas a adoptar en caso de transporte, reutilización o desecho de soportes y documentos — Identifica al encargado del tratamiento y los ficheros afectados y esto se expresa en el DS y en el contrato — Se debe mantener actualizado tanto en lo relativo a la organización como a la legislación vigente
Personal	— El Documento de Seguridad especifica las funciones y obligaciones de un modo claro y documentado — Se difunden entre el personal las normas que les afecten y las consecuencias por incumplimiento
Registro de incidencias	Se debe registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados
Control y registro de accesos	— Cada usuario accede únicamente a los datos y recursos necesarios para el desarrollo de sus funciones — Existe una relación actualizada de usuarios, perfiles y accesos autorizados — Existen mecanismos para controlar los derechos con que se accede a los recursos — Existen mecanismos que gestionen la concesión de permisos de acceso sólo por personal autorizado en el Documento de Seguridad

Gestión de soportes y documentos	— Se identifica el tipo de información que contienen. — Se mantiene un inventario — Se almacenan con acceso restringido — El responsable del fichero autoriza la salida de soportes — Se adoptan medidas en caso de desecho de soportes	
Criterios de archivo	Se debe garantizar la correcta conservación, localización y consulta de los documentos y posibilitar el ejercicio de los derechos ARCO	
Dispositivos de almacenamiento	Deben disponer de mecanismos que obstaculicen su apertura	
Custodia de soportes	**S**e debe custodiar la documentación cuando no se encuentre en archivada en los dispositivos de almacenamiento	
Responsable de seguridad		— Es el encargado de coordinar y controlar las medidas de seguridad del documento — Esto no supone exoneración de la responsabilidad del responsable del fichero
Auditoría		— Una interna o externa al menos cada 2 años o cuando se realicen cambios sustanciales en los SSII — Da lugar a un informe de auditoría sobre la adecuación a las medidas, las deficiencias identificadas y propone medidas correctoras — Es analizado por el responsable de seguridad — Queda a disposición de la AVPD

Almacenamiento de la información		Archivadores en áreas de acceso protegido con llave u otros sistema equivalente
Copia o reproducción		— Sólo personal autorizado en el DS — Las copias desechadas se deben destruir
Acceso a documentación		— Sólo personal autorizado — Existen mecanismos de identificación de accesos — Existe un registro de accesos no autorizados
Traslado de documentación		Se adoptan medidas para impedir el acceso o manipulación

ANEXO II.
SUPUESTOS CONCRETOS DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

SC I. Tratamiento de datos en la Investigación

En la Declaración de Ficheros de la UPV/EHU, aprobada en virtud de acuerdo adoptado por el Consejo de Gobierno de la Universidad de 8 de febrero de 2007, para la creación, modificación y supresión de ficheros de datos de carácter personal, publicado por Resolución de 28 de febrero de 2007 del Secretario General de la UPV/EHU (BOPV n.º 69, de 11 de abril de 2007), se crearon los siguientes tres ficheros genéricos relacionados con la Investigación: Investigación nivel básico, Investigación nivel medio e Investigación nivel alto.

No obstante, al margen de los ficheros genéricos, las acciones investigadoras que se desarrollan en la UPV/EHU puede que necesiten la creación de ficheros específicos. En este sentido, se establece que:

a) Si el fichero asociado a la acción investigadora tiene una duración inferior a un año, se integrará en alguno de los ficheros genéricos ya creados de nivel básico, medio o alto.
b) Si el fichero asociado a la acción investigadora tiene una duración superior a un año:
    b.1) Se creará un nuevo fichero específico para esa acción investigadora;
    b.2) Se integrará en alguno de los ficheros de investigación específicos que puedan estar ya declarados, (procediendo, si se introduce algún dato diferente respecto a los contenidos en el apartado n.º 5 de la

Si la acción investigadora implica un tratamiento de datos de carácter personal superior a un año, se procederá: bien a la creación de un nuevo fichero, bien a su integración en alguno de los ficheros de investigación ya declarados.

Declaración del fichero, a la modificación del fichero específico ya declarado para que dé cabida a la nueva acción investigadora).

Los investigadores que deseen llevar a cabo una acción investigadora valiéndose de datos de carácter personal, previamente al inicio de una acción investigadora, deberán contactar con el Vicerrectorado de Investigación con el objeto de fijar las pautas a respetar para el cumplimiento de lo establecido en el presente Reglamento.

SC II. Compromisos a asumir por empresas externas que realizan tratamientos de datos por cuenta de la UPV/EHU

La UPV/EHU contrata a múltiples empresas proveedoras de servicios con el objeto de dar respuesta a sus propias necesidades. Algunas de estas empresas para cumplir con el cometido que se les ha sido asignado deben acceder a datos de carácter personal de ficheros de la UPV/EHU; por ejemplo, las empresas de seguridad y las empresas que gestionan las bolsas de búsqueda de empleo. En consecuencia, la Universidad debe asegurarse en el contrato que se suscriba con tales empresas de que éstas van a respetar la normativa en materia de protección de datos de carácter personal.

Con las empresas que accedan a datos de carácter personal de ficheros de la UPV/EHU con el fin de prestar los servicios para los que hayan sido contratadas, se firmará un contrato que deberá contener, al menos, las cláusulas que se indican en este anexo.

Las siguientes cláusulas se incluirán en los contratos que se suscriban con empresas que deban a acceder a datos de carácter personal de ficheros de la UPV/EHU, es decir, que actúen como Encargados del tratamiento por cuenta de la Universidad:

Primera. Necesidad de acceso a los datos de carácter personal

Para la realización de los servicios objeto del presente contrato la UPV/EHU facilitará a la empresa adjudicataria el acceso a aquellos ficheros de datos de carácter personal que sea necesario, y ésta tratará dichos datos con el fin exclusivo de dar cumplimiento a los objetivos del contrato.

Segunda. Encargado de tratamiento

En conformidad lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, queda entendido que la empresa adjudicataria ostenta la condición de Encargado de tratamiento, esto es, persona jurídica que trata los datos por cuenta de la UPV/EHU, quien, como Responsable de fichero o tratamiento, decide la finalidad y el uso de la información a que tiene acceso la empresa adjudicataria.

Tercera. Instrucciones

La empresa adjudicataria únicamente tratará los datos conforme a las instrucciones de la UPV/EHU, no los aplicará o utilizará con fin distinto al que figura en el presente contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Cuarta. Cumplimiento de la normativa

La empresa adjudicataria conoce quedar obligada al respeto de los requerimientos y obligaciones que le correspondan en calidad de Encargado de tratamiento según se establece en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en cualquier otra disposición que en materia de protección de datos le fuera aplicable.

Quinta. Medidas de seguridad

La empresa adjudicataria se obliga a aplicar a los datos las medidas de seguridad que se establecen en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal, y que se correspondan con el nivel de seguridad de los ficheros a tratar. Asimismo, también queda obligada a aplicar aquellas medidas de seguridad que se encuentren en vigor o puedan estarlo durante la vigencia del presente contrato.

Sexta. Secreto profesional

La empresa adjudicataria observará en todo momento el secreto profesional y deber de confidencialidad sobre todos los datos recibidos de la UPV/EHU, obligándose a no revelar, transferir, ceder o comunicar de cualquier forma los datos a terceras personas, obligación que se mantendrá aún finalizada su relación con ésta. La empresa adjudicataria se compromete a comunicar y hacer cumplir a sus empleados las obligaciones establecidas en el presente contrato y, en concreto, las relativas al deber de secreto y medidas de seguridad.

Séptima. Finalización del contrato

Una vez cumplida la prestación contractual, la empresa adjudicataria destruirá los datos recibidos o los devolverá a la UPV/EHU, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento o contenga información sobre los ficheros recibidos.

SC III. Compromisos a asumir por empresas externas que en cumplimiento de las funciones asignadas por la UPV/EHU puedan entrar en contacto con datos en manos de la UPV/EHU

El personal de algunas empresas contratadas por la Universidad para la provisión de servicios que no implican tratamientos de carácter personal, al tener acceso a las instalaciones de la UPV/EHU, pueden tener acceso a información que puede contener datos de carácter personal. Tal circunstancia se da, por ejemplo, en el caso de las empresas de servicios de limpieza y reciclaje contratadas.

Los contratos que se firmen con las empresas, que en la prestación de sus servicios puedan entrar en contacto con datos en poder de la UPV/EHU, deben contener al menos las cláusulas indicadas en este anexo.

La UPV/EHU debe adoptar las medidas necesarias para garantizar que tales empresas no realicen un uso indebido de la información a la que tienen acceso y, por lo tanto, en el contrato a firmar con las mismas se incluirán, como mínimo, las siguientes cláusulas:

Primera. Acceso a locales de tratamiento

Para la realización de los servicios objeto del presente contrato en la Universidad del País Vasco/Euskal Herriko Unibertsitatea es necesario que personal de la empresa adjudicataria tenga acceso a locales donde se realizan tratamientos de ficheros con datos de carácter personal así como de otro tipo de documentación de carácter confidencial.

Segunda. Medidas de seguridad

El personal de la empresa adjudicataria queda obligado a respetar las medidas de seguridad de los locales a los que accede, sin que de su permanencia o paso por ellos pueda derivarse una merma de las condiciones de seguridad originales (cierre de puertas y ventanas, conexión de alarmas, etc.).

Tercera. Secreto profesional

El personal de la empresa adjudicataria deberá observar en todo momento el secreto profesional y deber de confidencialidad sobre todos los datos a los que pudiera tener acceso incidentalmente en el cumplimiento

de las tareas encomendadas. El personal de la empresa adjudicataria queda obligado a no revelar, transferir, ceder o comunicar de cualquier forma los datos a terceras personas, obligación que se mantendrá aún finalizada su relación con ésta. La empresa adjudicataria se compromete a comunicar y hacer cumplir a sus empleados las obligaciones establecidas en el presente contrato y, en concreto, las relativas al deber de secreto.

SC IV. Solicitudes de datos de carácter personal en manos de la UPV/EHU por entidades externas

En el caso de que una entidad externa solicite a la UPV/EHU datos de carácter personal en sus manos para cuya cesión a terceros se requiera el consentimiento de los interesados se podrá obrar de una de las dos maneras siguientes:

a) **Suscripción de un Convenio**

En el supuesto de que una entidad externa solicite a la UPV/EHU la cesión de datos de carácter personal en sus manos para un fin que la Universidad considere de interés de acuerdo con sus Estatutos, se deberá proceder a la tramitación del correspondiente convenio en función de lo establecido en la normativa universitaria aplicable.

Si una entidad externa solicita datos de carácter personal a la UPV/EHU, se puede optar por: a) firmar un convenio, tras asegurarse que se cuenta con el consentimiento de los titulares de los datos; b) asumir la distribución como propia de la UPV/EHU, si lo que se pretende es acorde con los fines universitarios y la Universidad lo considera de interés.

En la tramitación del convenio, se solicitarán informes a la persona Responsable de Seguridad LOPD y a la persona Responsable del fichero o tratamiento, los cuales serán vinculantes. Para que se pueda llevar a cabo la cesión, la persona Responsable del fichero o tratamiento deberá confirmar en su informe que las personas cuyos datos se solicitan han dado previamente el consentimiento para la cesión y, si no lo han hecho, solicitar dicha autorización, siguiendo alguna de las fórmulas establecidas en el artículo 12 del presente Reglamento.

El convenio a suscribir con la entidad externa deberá contener como mínimo las cláusulas siguientes:

> La entidad externa o Cesionaria tendrá que manifestar expresamente que cumple con la normativa de desarrollo vigente en materia de protección de datos de carácter personal, y asumirá los siguientes compromisos:
>
> 1. Tratar los Datos que se le ceden con la finalidad exclusiva de [introducir finalidad con detalle y su duración en el tiempo, en principio para un único momento y durante un plazo de tiempo determinado].

Cualquier tratamiento de los datos que no se ajuste a la finalidad para la que son cedidos, será responsabilidad exclusiva de la Cesionaria, que responderá frente a terceros y frente a la propia Universidad de los daños y perjuicios que pudieren generarse.

2. Ejercitado el derecho de cancelación de datos por parte de las personas interesadas o cuando la Universidad lo estime oportuno y así lo comunique a la Cesionaria, cesar de inmediato en el tratamiento de los datos y proceder a la supresión de los mismos.
3. Aplicar a los Datos las medidas de seguridad previstas en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como lo dispuesto en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal. El incumplimiento de este compromiso será responsabilidad exclusiva de la Cesionaria que responderá frente a terceros y frente a la propia Universidad de los daños y perjuicios que pudieran generarse.
4. No realizar ninguna cesión de los datos que le son cedidos.
   La persona Responsable del fichero o tratamiento procederá al registro de las cesiones de datos realizadas, con el fin de garantizar el efectivo futuro ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los interesados. Asimismo, las cesiones realizadas serán reflejadas en el correspondiente Registro de entradas y salidas del Documento de Seguridad del fichero.

b) **Asumir la distribución de la información de la entidad externa**

Como salvedad al procedimiento establecido en los apartados anteriores, si se recibe una solicitud de datos por parte de una entidad externa y la UPV/EHU considere de interés colaborar en la divulgación de determinada información facilitada por la entidad externa (interés el cual siempre tendrá que estar relacionado con los fines de la UPV/EHU según sus Estatutos), la Universidad podrá llevar a cabo dicha distribución y correr con los gastos.

La unidad organizativa de la UPV/EHU implicada (Rectorado, Vicerrectorados, Gerencia, Centros, Institutos y Cátedras), tras la correspondiente aprobación de la iniciativa por su máxima persona responsable, solicitará el permiso

correspondiente a la persona Responsable de Seguridad LOPD. Una vez de haber recibido la autorización por escrito de la persona Responsable de Seguridad LOPD, la unidad organizativa interesada se encargará del envío de la información facilitada por la entidad externa, la cual irá introducida por un escrito de presentación de la Universidad que justifique el interés de dicho envío.

El medio prioritario de distribución será el correo electrónico. Tan sólo en supuestos excepcionales, debidamente justificados en la solicitud que se realice a la persona Responsable de Seguridad LOPD, se procederá al envío por correo postal.

Asimismo, se podrán habilitar en la web de la Universidad lugares en los que se pueda colocar información no directamente relacionada con la Universidad pero de interés para la comunidad universitaria, conforme al procedimiento que se establezca al efecto.

SC V. Solicitudes de datos de autoridades judiciales, policiales y administrativas

1. La información sobre datos de carácter personal obrantes en ficheros de la UPV/EHU que puede afectar a alumnado, personal o terceros, será comunicada a autoridades judiciales, policiales y administrativas, con sujeción al procedimiento legalmente establecido y a las reglas que se exponen a continuación. No se atenderán peticiones de información sobre datos de carácter personal no motivadas. La cesión de datos a autoridades judiciales, policiales y administrativos será supervisada por la persona Responsable del fichero o tratamiento y la persona Responsable de Seguridad LOPD.

2. En el momento en que se obtenga una solicitud de de datos por parte de autoridades judiciales, policiales y administrativas, se contactará con el Servicio Jurídico de la Universidad. No se procederá a la remisión de ninguna información sin el previo visto bueno del Servicio Jurídico. El Servicio Jurídico se encargará de contactar con la persona Responsable del fichero o tratamiento y la persona Responsable de Seguridad LOPD. No se procederá a la entrega de ningún dato sin el previo visto bueno del Servicio Jurídico.

Cuando se reciba una solicitud de datos por parte de autoridades judiciales, policiales o administrativas, se debe contactar con el Servicio Jurídico de la Universidad.

3. Las solicitudes realizadas por autoridades judiciales, se facilitarán en la medida en que sean solicitadas mediando la intervención del juez. Las informaciones solicitadas por órganos gubernativos directamente relacionados con actuaciones preparatorias o complementarias de procesos judiciales, serán facilitadas cuando conste claramente la intervención de órgano judicial concreto.

4. En relación con las solicitudes realizadas por las autoridades policiales, los ficheros policiales tienen una regulación especial contenida dentro del artículo 22 de la LOPD y en base a ella, la recogida y tratamiento para fines policiales de datos de carácter personal manejados por centros públicos de enseñanza, por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de

su grado de fiabilidad. Este artículo habilita a las Fuerzas y Cuerpos de Seguridad para la obtención y tratamiento de los datos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando se cumplan las siguientes condiciones:

a) que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales;
b) que se trate de una petición concreta y específica, al no ser compatible con lo señalado el ejercicio de solicitudes masivas de datos;
c) que la petición se efectúe con la debida motivación, que acredite su relación con lo supuestos que se han expuesto;
d) que los datos sean cancelados cuando dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento, en cumplimiento del artículo 22.4 de la LOPD.

5. Se facilitarán los datos solicitados por autoridades administrativas cuando:

a) la solicitud haya sido presentada por la Inspección Tributaria, la Agencia Estatal Tributaria, las Haciendas Forales de los Territorios Históricos o las Oficinas Recaudatorias de las Haciendas Locales, en virtud de lo establecido en los artículos 111 y 112 de la Ley General Tributaria, el artículo 37 del Reglamento General de Inspección de Tributos, y la correspondiente normativa foral, o normativa vigente en cada momento y siempre que la información solicitada tenga trascendencia tributaria;
b) la solicitud sea presentada por el Instituto Nacional de la Seguridad Social o cualquiera de sus Agencias, en el ejercicio de las competencias que le son propias;
c) la solicitud sea presentada por la autoridad laboral correspondiente en el uso de las competencias que le son propias;
d) la solicitud de datos se presente basada en la Ley 12/1989, de 12 de mayo, sobre Función Pública Estadística y la Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma del País Vasco, para la elaboración de estudios de este carácter;
e) siempre que las cesiones sean obligatorias en virtud de una ley.

SC VI. Prestación de servicios por parte de la UPV/EHU a entidades externas

Las siguientes cláusulas se incluirán en los convenios/contratos que se suscriban con empresas/entidades cuando la Universidad actúe como Encargada del tratamiento de datos de carácter personal por cuenta de terceros.

La normativa de protección de datos de carácter personal cuando ha ser también respetada cuando la Universidad preste servicios a terceros (por ejemplo, vía contratos del artículo 83 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades).

Primera. Necesidad de acceso a los datos de carácter personal

Para la realización de los servicios objeto del presente convenio/contrato la (entidad o empresa con quien se subscribe el convenio o contrato), facilitará a la UPV/EHU el acceso a aquellos ficheros de datos de carácter personal que sea necesario, y esta tratará dichos datos con el fin exclusivo de dar cumplimiento a los objetivos del convenio/contrato.

Segunda. Encargado de tratamiento

En conformidad lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal con, queda entendido que la UPV/EHU ostenta la condición de Encargado de tratamiento, esto es, la persona jurídica que trata los datos por cuenta de (la entidad o empresa con quien se subscribe el convenio o contrato), quien, como responsable de fichero, decide la finalidad y el uso de la información a que tiene acceso la UPV/EHU.

Tercera. Instrucciones

La UPV/EHU únicamente tratará los datos conforme a las instrucciones que de (la entidad o empresa con quien se subscribe el convenio o contrato), no los aplicará o utilizará con fin distinto al que figura en el presente convenio/contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Cuarta. Cumplimiento de la normativa

La (entidad o empresa con quien se subscribe el convenio o contrato), conoce quedar obligada al respeto de los requerimientos y obli-

gaciones que le correspondan en calidad de Responsable de fichero o tratamiento según se establece en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en cualquier otra disposición que en materia de protección de datos le fuera aplicable, en particular, de la obligación de tener declarados los ficheros ante la Agencia de Protección de Datos correspondiente, así como en cualquier otra disposición que en materia de protección de datos le fuera aplicable.

Quinta. Medidas de seguridad

La UPV/EHU se obliga a aplicar a los datos las medidas de seguridad que se establecen en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal, y que se correspondan con el nivel de seguridad de los ficheros a tratar. Así mismo, también queda obligada a aplicar aquellas medidas de seguridad que se encuentren en vigor o puedan estarlo durante la vigencia del presente contrato.

Sexta. Secreto profesional

La UPV/EHU observará en todo momento el deber de confidencialidad sobre todos los datos recibidos de (la entidad o empresa con quien se subscribe el convenio o contrato), obligándose a no revelar, transferir, ceder o comunicar de cualquier forma los datos a terceras personas, obligación que se mantendrá aún finalizada su relación con ésta. La UPV/EHU se compromete a comunicar y hacer cumplir a sus empleados las obligaciones establecidas en el presente convenio/contrato y, en concreto, las relativas al deber de secreto y medidas de seguridad.

Séptima. Finalización del contrato

Una vez cumplida la prestación contractual, la UPV/EHU destruirá los datos recibidos o los devolverá a (la entidad o empresa con quien se subscribe el convenio o contrato), al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento o contenga información sobre los ficheros recibidos.

SC VII. Publicidad de notas de exámenes

La publicación de notas de exámenes se llevará a cabo en los tablones de anuncios mediante la identificación del alumnado únicamente con su DNI.

Los listados para dar publicidad de notas de exámenes se mantendrán durante el tiempo necesario para cumplir su finalidad de publicidad, que nunca podrá ser superior a un mes, y permitir el ejercicio de los derechos del alumnado.

Las notas de los exámenes deben ser publicadas indicando solamente el DNI. Los listados de resultados de exámenes tienen que contener la cláusula informativa correspondiente.

Los mencionados listados incorporarán una cláusula advirtiendo lo siguiente:

Este listado contiene datos de carácter personal, se ajusta a la normativa actual en materia de protección de datos y su única finalidad es la dar publicidad al presente proceso de evaluación. No constituye fuente de acceso público y no podrá ser reproducido ni en todo ni en parte, ni transmitido ni registrado por ningún sistema de recuperación de información, sin el consentimiento de los propios afectados.

La publicidad de notas de exámenes del alumnado en páginas Web sólo se realizará con un control de acceso mediante clave que impida su consulta a personas distintas a la persona interesada.

SC VIII. Procesos de concurrencia competitiva

La publicidad de los listados provisionales y definitivos en los procesos de concurrencia competitiva con independencia del medio en que se hagan públicos (tablón de anuncios, página web...), contendrán los datos de carácter personal mínimos necesarios para cumplir el principio de publicidad (nombre, apellidos y DNI) y se mantendrán hasta la finalización del correspondiente proceso y durante el tiempo adicional necesario para el ejercicio de las reclamaciones o recursos.

En determinados procesos, el órgano competente podrá optar por restringir la publicación de datos de carácter personal al DNI.

En los procesos de concurrencia competitiva de carácter universitario tales como convocatorias de becas, bolsas y ayudas, y prácticas, bastará con el nombre y apellidos.

Los mencionados listados incorporarán una cláusula advirtiendo que:

Los resultados en los procesos de concurrencia competitiva indicarán el nombre, apellidos y DNI de los interesados. Dichos listados contendrán la cláusula informativa correspondiente.

Este listado contiene datos de carácter personal, se ajusta a la normativa actual en materia de protección de datos y su única finalidad es la dar publicidad al presente proceso de selección. No constituye fuente de acceso público y no podrá ser reproducido ni en todo ni en parte, ni transmitido ni registrado por ningún sistema de recuperación de información, sin el consentimiento de los propios afectados o afectadas.

SC IX. Obtención de datos del alumnado por parte del profesorado

Al inicio de cada curso los datos de carácter personal que el profesorado necesita saber de su alumnado, incluida su fotografía, estarán disponibles a través del sistema informático de gestión académica de la Universidad.

El profesorado no puede solicitar al alumnado la entrega de fichas manuales. El sistema informático de gestión académica proporciona suficiente información.

Por lo tanto, no se permite el sistema tradicional de fichas manuales que hasta la fecha eran solicitadas por el profesorado al inicio de cada curso.

En el momento de hacer la matrícula se informará al alumnado de la finalidad y uso que se va a realizar de su fotografía.

SC X. Página web corporativa

1. Las páginas web de la UPV/EHU de acceso libre no deben contener datos de carácter personal salvo que se cumplan las siguientes condiciones:

a) Correspondan a ficheros declarados por la UPV/EHU.
b) Y el titular posea consentimiento expreso para su publicación otorgado por las personas cuyos datos son mostrados en la página.

2. No se publicarán listas de grupos de alumnado (de asignaturas, de prácticas, etc.) salvo en los siguientes supuestos

a) Sólo puedan acceder las personas interesadas mediante un proceso de autenticación.
b) Las personas afectadas hayan dado su consentimiento al procedimiento de publicación de listas.

No se permite publicar listados de alumnado en páginas web de libre acceso, salvo previo consentimiento de los afectados.

3. Cuando se recaben datos de carácter personal con una finalidad determinada, debe informarse a la persona interesada de los extremos mencionados en el artículo 7.1 del presente Reglamento.

4. Las páginas web de la UPV/EHU deben cumplir rigurosamente, en lo que les afecte, la política de privacidad de la Universidad, la cual se publicita en el portal corporativo en el apartado relativo a «Información Legal» bajo el epígrafe «Política de protección de datos de carácter personal»:

> 1. La UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA pone en conocimiento de los usuarios de este sitio que podrá crear un archivo automatizado con los datos de carácter personal que sean facilitados a la misma como consecuencia de la utilización del presente sitio web y en estricto cumplimiento con lo preceptuado en la normativa en materia de protección de datos de carácter personal.
>
> 2. Los usuarios garantizan la veracidad y autenticidad de las informaciones y datos que comuniquen en virtud de la utilización de este sitio web. En este sentido, será de obligación de los usuarios el mantener actua-

lizados las informaciones y datos de forma tal que correspondan a la realidad en cada momento. Cualquier manifestación falsa o inexacta que se produzca como consecuencia de las informaciones y datos manifestados así como los perjuicios que tal información pudiera causar será responsabilidad de los usuarios.

3. En cumplimiento de lo dispuesto en la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa que los datos de carácter personal serán recopilados y archivados en un fichero de datos cuyo responsable es la Gerencia de la UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA.

4. Los usuarios podrán ejercitar, en cualquier momento, los derechos de acceso, rectificación, cancelación y oposición de sus datos recopilados y archivados. El ejercicio de estos derechos deberá efectuarse mediante comunicación escrita dirigida a la persona Responsable de seguridad LOPD de la UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA. El ejercicio de estos derechos no afectara en modo alguno al acceso a la página web ni, en su caso, a la condición de abonado del usuario.

5. Los datos registrados podrán ser utilizados con la finalidad de efectuar estadísticas, la remisión de información científica, la gestión de incidencias o la realización de estudios de mercado, además de para las que expresamente se hayan recabado los datos.

6. En su caso, los datos de carácter personal facilitados por los usuarios podrán ser comunicados a un tercero sólo para el cumplimiento de los fines señalados anteriormente, ajustándose a lo establecido en los artículos 11 y 21 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, recabándose, en todo caso, el consentimiento de los interesados cuando este sea necesario.

7. Al facilitar los datos de carácter personal a la UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA, los usuarios declaran aceptar plenamente y sin reservas el tratamiento de los mismos por parte de la UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA.

8. La UNIVERSIDAD DEL PAÍS VASCO/EUSKAL HERRIKO UNIBERTSITATEA se compromete a cumplir con la obligación de guardar secreto respecto de los datos de carácter personal objeto de tratamiento y declara su intención de poner en práctica las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar 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.

SC XI. Directorio web

En el Directorio web de la UPV/EHU se encuentran los datos de identificación y contacto de todo el personal al servicio de la Universidad. Para garantizar, por una parte, la posibilidad de comunicación entre los distintos miembros de la comunidad universitaria se posibilita efectuar las consultas autenticándose la persona que las realiza, siendo visibles en ese supuesto todos los datos de identificación y contacto del personal; por otra parte, para permitir el derecho de las personas de que sus datos no sean consultados por cualquier persona ajena a la comunidad universitaria se permite a través del propio sistema de autenticación ocultar hacía el exterior los datos de identificación y contacto que se quieran restringir.

En el Directorio web, las consultas autenticadas posibilitan el acceso a los datos de identificación y contacto completos de los miembros de la comunidad universitaria.

SC XII. Cesión de datos en la vigilancia y protección de las condiciones de trabajo

La función de vigilancia y protección de las condiciones de trabajo, atribuidas a los distintos órganos de representación de los trabajadores puede llevarse a adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en la UPV/EHU.

No obstante lo anterior, en el caso de que la vigilancia o control se refieran a un sujeto particular, que haya planteado el problema concreto, será posible la cesión del dato específico de dicha persona.

En los demás supuestos, la función de control quedará plenamente satisfecha mediante la cesión de información de manera agregada o, en su caso, debidamente disociada, es decir, sin poder referenciar los datos a personas identificadas o identificables, que permita a aquélla conocer las circunstancias cuya vigilancia le ha sido encomendada sin referenciar la información en un sujeto concreto.

La cesión de datos a los representantes de los trabajadores para el cumplimiento de su función de vigilancia y protección de las condiciones de trabajo será realizada, en principio, de manera agregada o disociada.

Si se llegan a ceder datos de carácter personal a representantes de los trabajadores se indicará en dicha comunicación el deber de secreto que obliga a las personas que conozcan dicho dato.

SC XIII. Cesión de datos en materia de prevención de riesgos laborales

El artículo 30.3 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales señala lo siguiente: «*para la realización de la actividad de prevención, el empresario deberá facilitar a los trabajadores designados el acceso a la información y documentación a que se refieren los artículos 18 y 23 de la presente ley*».

El artículo que se refiere a la documentación es el 23 que recoge lo siguiente:

> 1. El empresario deberá elaborar y conservar a disposición de la autoridad laboral la siguiente documentación relativa a las obligaciones establecidas en los artículos anteriores:
>
> a) Plan de prevención de riesgos laborales, conforme a lo previsto en el 16.1 de esta Ley.
> b) Evaluación de los riesgos para la seguridad y la salud en el trabajo, incluido el resultado de los controles periódicos de las condiciones de trabajo y de la actividad de los trabajadores, de acuerdo con lo dispuesto en el párrafo a) del artículo 16.2 de esta Ley.
> c) Planificación de la actividad preventiva, incluidas las medidas de protección y de prevención a adoptar y, en su caso, material de protección que deba utilizarse, de conformidad con el párrafo b) del artículo 16.2 de esta Ley.
> d) Práctica de los controles del estado de salud de los trabajadores previstos en el artículo 22 de esta Ley y conclusiones obtenidas de los mismos en los términos recogidos en el último párrafo del apartado 4 del citado artículo.
> e) Relación de accidentes de trabajo y enfermedades profesionales que hayan causado al trabajador una incapacidad laboral superior a un día de trabajo. En estos casos el empresario realizará, además, la notificación a que se refiere el apartado 3 del presente artículo.

Aquellos que tengan acceso a datos de carácter personal en cuestiones de prevención de riesgos laborales, están obligados a cumplir con el deber de sigilo profesional.

De la relación transcrita se entiende que se pueden cumplir los objetivos de la ley a través de información agregada. No obstante, en el supuesto de que la citada documentación deba contener datos de carácter personal, o que con ocasión de las actuaciones que desarrollen se conozcan determinados datos de carácter personal, se deberá cumplir con el deber de sigilo que le impone el artículo 37.3 de la ley.

SC XIV. Referencias personales

En el contexto del presente Reglamento, el término «referencias personales» alude a las acciones de solicitar y dar información sobre alumnado o egresados, generalmente a modo de recomendaciones, con fines laborales o de perfeccionamiento profesional. La provisión de referencias implica usualmente la comunicación de datos de carácter personal.

La revisión de la política y la práctica en relación a las referencias personales es una operación básica para la adecuación a la normativa legal en materia de datos de carácter personal. Por ello, la UPV/EHU en el futuro podrá establecer una política institucional sobre referencias personales, en la cual se identifique quién puede facilitar referencias en nombre de la organización, cómo manejar las peticiones de referencias, tipos de información que pueden ser proporcionados, cómo se articula la concesión de acceso a las mismas, etc. La UPV/EHU se asegurará que todas las personas que pudieran recibir una petición de referencias conocen estas recomendaciones y, en su caso, la política sobre referencias elaborada.

Cómo proporcionar referencias

Cuando una persona, en su calidad de futura empleadora o para conceder becas u otras oportunidades de enriquecimiento profesional, solicita que se le facilite la identidad de alumnado o egresados que cumplen un determinado perfil o, por otro lado, solicita de una determinada persona de la UPV/EHU que proporcione datos evaluativos sobre alumnado o egresados concretos, se ha de cumplir el siguiente protocolo:

1. Informar que existen espacios (denominados actualmente PRAKTIGES y LANBILA) destinados a que las entidades anuncien sus oportunidades de empleo, planes de formación o profesionales, etc., de tal manera que la totalidad del colectivo potencialmente interesado puede enviar su candidatura a la oferta u oportunidad que se anuncia.
2. Las referencias se considerarán realizadas en nombre de la UPV/EHU, por lo que la personal que realiza las referencias tendrá que ser consciente de que lo hace como integrante de la Universidad.
3. Informar de quién puede facilitar referencias sobre alumnado o egresados en nombre de la UPV/EHU en las distintas estructuras y unidades organizativas de la Universidad, a decisión de éstas. Sobre esta cuestión, el principio que ha de aplicarse es que las personas que pueden evaluar a otras son aquéllas que tienen formalmente competencias evaluadoras y

que han tenido, en términos comparativos, más y mejores oportunidades para medir algunas competencias generales o específicas de un alumno o alumna o de un grupo de alumnos. En este sentido, las personas más capacitadas para evaluar a alumnado o egresados podrán ser sus tutores, profesorado de prácticas o personas que hayan mantenido una relación cercana y continuada en el tiempo con el alumno o alumna durante el proceso de enseñanza-aprendizaje.

4. Todas las personas que dan referencias a terceros en nombre de la UPV/EHU deben asegurarse de que la persona objeto de las referencias desea que sean facilitadas, esto es, deberá obtenerse previamente su consentimiento.
5. La persona que proporcione las referencias deberá remitir una copia de las mismas a la Secretaría del Centro, o estructura que corresponda, para que sea archivado junto al expediente académico.
6. Toda referencia sobre alumnado o egresados ha de basarse en una medición y evaluación de competencias o recursos de competencias de los mismos que resulte útil, viable y bien fundamentada, de conformidad con los estándares de evaluación de personas y evaluación de programas aceptados comúnmente por la comunidad científica en su aplicación al campo educativo.
7. Las referencias deben elaborarse con la asunción de que el titular del dato tendrá la oportunidad de ver lo que se ha escrito sobre él. El derecho del individuo a conocer lo que se ha escrito acerca de él incrementa la robustez del proceso de elaboración de una referencia.
8. No se recomienda la emisión de referencias orales y, en todo caso, para la emisión de las mismas será necesaria la obtención del consentimiento previo de las personas afectadas. La UPV/EHU no será responsable de las referencias orales que puedan ser emitidas por su personal, debido a los problemas derivadas de su falta de calidad en el tratamiento de los datos de carácter personal y la posible pérdida de fiabilidad y validez de los datos evaluativos.

Para facilitar referencias a terceros se necesita la obtención del consentimiento del titular de los datos. Dichas referencias serán archivadas junto al expediente académico del alumno o alumna.

Cómo dar acceso a una persona a sus propias referencias

El evaluador o evaluadora de un alumno o alumna, que haya emitido una referencia con el consentimiento de la persona implicada, no está obligado a proveer una copia de la misma a la persona de la que trata la misma. El alumno o alumna que desea conocer las referencias emitidas sobre su persona podrá tener acceso a sus referencias acudiendo a la Secretaría del Centro o estructura que corresponda.

El alumnado tendrá derecho a solicitar la cancelación de las referencias sobre su persona archivadas junto con su expediente académico ejerciendo el derecho de cancelación de las mismas.

SC XV. Evaluación de la actividad docente

Según la normativa universitaria (siendo la más importante al respecto la relativa a la evaluación de la docencia prevista en el artículo 160.2 de los Estatutos de la UPV/EHU), con las cautelas que procedan para garantizar los derechos de los interesados, y con sujeción a los principios de racionalidad, rigor, confidencialidad y objetividad, los resultados de las encuestas relativas a la evaluación de la docencia de carácter individual o, en su caso, agrupados como corresponda, serán comunicados al profesorado, a los Departamentos, a los centros docentes y a los representantes del alumnado a fin de que se realicen las valoraciones oportunas de cara a la mejora de las enseñanzas y sin perjuicio de que se puedan formular las alegaciones que correspondan.

Con las cautelas que procedan, los resultados de las encuestas relativas a la evaluación de la docencia de carácter individual serán comunicados a los interesados.

En todo caso, el Profesorado, los Departamentos, los Centros Docentes y los representantes del alumnado podrán acceder a los resultados agregados de las evaluaciones del profesorado en las que se cumpla la condición de interesado.

Asimismo, dichas instancias podrán solicitar resultados de carácter individual de las encuestas relativas a la evaluación de la docencia en supuestos debidamente justificados tales como: solicitudes de los Departamentos y centros docentes realizadas por sus órganos colegiados de representación con el fin de realizar análisis encaminados a la mejora de las enseñanzas que imparten.

Junto con el envío de la documentación que soliciten se les deberá recordar que la información que reciben no es pública y que por tanto, deben guardar sigilo sobre su contenido. En el caso de incumplimiento de tal deber de secreto, responderán disciplinariamente por la falta cometida.

SC XVI. Cláusula tipo para matrícula

Protección de datos: De acuerdo con lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que sus datos pasan a formar parte de los ficheros de la UPV/EHU cuya finalidad esté relacionada con sus estudios universitarios.

Puede ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos remitiendo un escrito a la persona Responsable de Seguridad LOPD de la UPV/EHU, Rectorado, Barrio Sarriena s/n, 48940 Leioa-Bizkaia, adjuntando copia de documento que acredite su identidad.

Se consultará a la persona «Responsable de Seguridad LOPD» cuando se quiera introducir cláusulas adicionales relativas a la obtención del consentimiento para la cesión de datos.

De forma potestativa, los centros universitarios podrán incluir otras cláusulas supervisadas previamente por la persona Responsable de Seguridad LOPD con el objeto de recabar el consentimiento del alumnado para la cesión de sus datos personales a entidades terceras relacionadas con fines universitarios.

SC XVII. El derecho de acceso y la protección de datos de la documentación en papel

Se considera documento administrativo toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogida en cualquier tipo de soporte material, que es testimonio de las actividades propias de una organización en el cumplimiento de sus fines.

En este apartado nos vamos a referir a los documentos en soporte papel, que forman parte del Patrimonio Documental de la Universidad del País Vasco/Euskal Herriko Unibertsitatea, generados por cualquiera de su órganos de Gobierno y Administración, así como por sus Órganos de Representación, Departamentos, Escuelas, Facultades e Institutos Universitarios en el desempeño de sus funciones.

Consulta y préstamo de la documentación custodiada por el Archivo General

La difusión de la información, junto con la conservación, son los objetivos de todo Archivo.

El Archivo General de la Universidad del País Vasco/Euskal Herriko Unibertsitatea respetará siempre la legislación sobre el Derecho de Acceso a Archivos y Registros recogida en la Constitución y la Ley 30/1992, de 26 de noviembre, de las Administraciones Públicas y del Procedimiento Administrativo Común, la Ley 9/1968, de 5 de abril, reguladora de los Secretos Oficiales, la legislación sobre protección de datos de carácter personal, y lo recogido en el Reglamento de la UPV/EHU para la Protección de Datos de Carácter Personal.

Será la Comisión de Valoración y Expurgo o Comisión de Archivo de la Universidad (creada mediante Acuerdo del Consejo de Gobierno de la UPV/EHU, de 21 de julio de 2005, publicado en el BOPV n.º 170, de 7 septiembre de 2005), la que decida el plazo que deba transcurrir para la libre consulta de la documentación custodiada en el mismo.

La consulta de documentos de acceso restringido podrá llevarse a cabo mediante consulta directa en las instalaciones habilitadas al efecto en el Archivo General previa autorización del Secretario General.

Se prestará la documentación que las unidades administrativas productoras soliciten, siempre que haya transcurrido un tiempo mínimo, desde su transferencia al Archivo, que haya permitido su integración en el conjunto documental.

Cuando una unidad administrativa necesite un expediente, habrá de hacer la solicitud por escrito haciendo constar en el formulario de préstamo los datos fun-

damentales para su identificación. Sólo se prestarán documentos a la unidad que los haya generado.

En el caso de que una unidad solicite documentos de acceso restringido originados por otra, el préstamo se hará a la unidad generadora, quien decidirá a su vez si procede o no el préstamo.

Las solicitudes de expedientes que constan en el Archivo las realizará por escrito la unidad administrativa que los haya generado.

Desde el Archivo se facilitarán los formularios de préstamo, que constarán de un original y una copia. La copia se entregará a la unidad solicitante junto con la documentación, mientras que el original quedará en el Archivo dentro de la carpeta de préstamos pendientes. La persona que firme el formulario de préstamo será responsable de que la consulta se haga respetando la legislación de protección de datos de carácter personal y su normativa de desarrollo.

Reprografía de documentos de acceso restringido

Para la reproducción de documentos de acceso restringido será necesaria la autorización del Secretario General. En el caso de documentación con valor administrativo, el solicitante deberá dirigirse directamente a la unidad administrativa responsable del procedimiento.

Garantías en cuanto a las instalaciones y la conservación de los documentos

El Archivo contará con los locales e instalaciones adecuados para el depósito y la preservación de la documentación, así como para la realización de los procesos técnicos que suponen el tratamiento documental.

Para asegurar la integridad de la documentación custodiada por el Archivo General, no podrán acceder a sus depósitos personas no adscritas al mismo. Cualquier otro tipo de visita deberá contar con la autorización expresa del Secretario General.

Se establecerá un programa de documentos esenciales y se elaborará un Plan de emergencia para actuar en caso de catástrofes y siniestros.

Eliminación de la documentación en las oficinas

La eliminación de documentos en las diferentes unidades administrativas de la Universidad debe hacerse de manera controlada, preservando en todo momento el derecho al honor, a la intimidad y a la propia imagen de las personas cuyos datos estén contenidos en ellos.

Para ello, se recomienda utilizar una máquina destructora. En ningún caso se llevarán documentos que contengan datos personales al contenedor. Hay que proteger en todo momento los datos de carácter personal que puedan contener.

En caso de no disponer de los medios necesarios, deberán ponerse en contacto con el Archivo General para que se les facilite unas pautas de actuación.

Eliminación de la documentación en los Archivos Centrales o Intermedios

La eliminación o expurgo de la documentación custodiada en los Archivos Centrales o Intermedios, que forma parte del patrimonio documental de la Universidad, deberá ser aprobada por el Consejo de Gobierno de la Universidad a propuesta de la Comisión de Valoración y Expurgo o Comisión de Archivo de la Universidad.

Se levantará acta del expurgo, recogiéndose el compromiso por parte de la empresa encargada del mismo de la destrucción total de la documentación de manera que sea imposible la recuperación de ningún dato de carácter personal.