



# **CÓDIGO TIPO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA**

**(Aprobado por el Comité de Seguridad de la Información el 22 de febrero de  
2017 y por el Consejo de Gobierno de la UNED el 27 de junio de 2017)**

# ÍNDICE

<u>INTRODUCCIÓN</u> .....	4
<u>1. OBJETIVO DEL CÓDIGO TIPO</u> .....	4
<u>2. CONTENIDO DEL CÓDIGO TIPO</u> .....	5
<u>2.1. MARCO NORMATIVO</u> .....	5
<u>2.2. DEFINICIONES</u> .....	6
<u>2.3. ÁMBITO DE APLICACIÓN</u> .....	8
<u>2.4. ENTRADA EN VIGOR</u> .....	8
<u>2.5. OBLIGACIONES POSTERIORES A LA INSCRIPCIÓN DEL CÓDIGO TIPO</u> .....	8
<u>2.6. PRINCIPIOS DE LA PROTECCIÓN DE DATOS</u> .....	9
<u>2.6.1. Calidad de los datos</u> .....	9
<u>2.6.2. Derecho de información en la recogida de datos</u> .....	10
<u>2.6.3. Consentimiento del afectado</u> .....	11
<u>2.6.4. Principio de seguridad de los datos</u> .....	12
<u>2.6.5. El deber de secreto en el tratamiento de datos</u> .....	12
<u>2.6.6. Datos especialmente protegidos</u> .....	13
<u>2.6.7. Comunicación de datos</u> .....	13
<u>2.6.7.1. Comunicación de datos personales por parte de la UNED</u> .....	15
<u>2.6.7.2. Las transferencias internacionales de datos</u> .....	16
<u>2.6.8. Las prestaciones de servicios con y sin acceso a datos de carácter personal</u> .....	16
<u>2.6.8.1. Prestaciones de servicios con acceso a datos</u> .....	16
<u>2.6.8.2. Prestaciones de servicios sin acceso a datos</u> .....	17
<u>2.7. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN</u> .....	18
<u>2.7.1. Aspectos comunes</u> .....	18
<u>2.7.2. El derecho de acceso</u> .....	19
<u>2.7.3. El derecho de rectificación</u> .....	20
<u>2.7.4. Derecho de cancelación</u> .....	20

2.7.5. <a href="#">Derecho de oposición</a> .....	21
2.8. <a href="#">ACCIONES FORMATIVAS EN MATERIA DE PROTECCIÓN DE DATOS</a> .....	21
2.9. <a href="#">GESTIÓN DE LOS FICHEROS DE DATOS DE CARÁCTER PERSONAL</a> .....	22
2.9.1. <a href="#">Procedimiento interno de detección de ficheros en la UNED</a> .....	22
2.9.2. <a href="#">Procedimiento de declaración de ficheros LOPD</a> .....	22
2.10. <a href="#">MEDIDAS DE SEGURIDAD APLICABLES SOBRE LOS TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL</a> .....	25
2.10.1. <a href="#">Medidas de seguridad</a> .....	25
2.10.2. <a href="#">Auditorías de cumplimiento</a> .....	26
2.10.3. <a href="#">Ficheros temporales</a> .....	27
2.10.4. <a href="#">El documento de seguridad</a> .....	27
2.11. <a href="#">ROLES Y RESPONSABILIDADES</a> .....	28
2.12. <a href="#">LA COMISIÓN DE CONTROL DEL CÓDIGO TIPO</a> .....	29
2.13. <a href="#">PRESENTACIÓN DE SUGERENCIAS, QUEJAS O RECLAMACIONES</a> .....	30
2.14. <a href="#">INFRACCIONES Y SANCIONES</a> .....	31
2.15. <a href="#">PROCEDIMIENTO SANCIONADOR</a> .....	32
2.16. <a href="#">DIFUSIÓN Y EVALUACIÓN DE LA SATISFACCIÓN</a> .....	32
2.17. <a href="#">MEMORIA DE ACTIVIDADES</a> .....	33
ANEXOS .....	34

## **INTRODUCCIÓN**

En la sociedad de nuestros días vivimos en un universo digital de datos. La proliferación de ordenadores, teléfonos inteligentes y la vertiginosa evolución de Internet han tenido como consecuencia una expansión sin precedentes de los datos de carácter personal que se gestionan. Por lo tanto, una Universidad del siglo XXI, como la nuestra, tiene que afrontar este hecho.

La Universidad Nacional de Educación a Distancia (UNED) es la mayor de España, y cuenta con más de 183.000 estudiantes que cursan sus titulaciones oficiales (27 grados, 73 másteres universitarios así como 19 programas de doctorado) o sus más de 500 cursos de Formación Permanente.

Nuestra Universidad posee una de las bases de datos personales más importantes del país, la de los estudiantes que a lo largo de su historia han pasado por esta institución. Conocer la normativa de protección de datos es uno de los pilares de la gestión de calidad de la que se puede denominar Universidad electrónica.

La UNED tiene entre sus objetivos garantizar la protección de los datos de carácter personal de todas aquellas personas que con ella se relacionan: estudiantes, profesores, personal de administración y servicios y, en general, cualquier otro ciudadano que en algún momento de su vida tenga relación con nuestra institución.

### **1. OBJETIVO DEL CÓDIGO TIPO**

Los códigos tipo constituyen un instrumento de lo que se denomina autorregulación, es decir, la capacidad de las organizaciones y entidades para regularse a sí mismas. En el ámbito de la protección de datos de carácter personal esa capacidad está orientada a la adopción de reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por quienes se adhieran al código tipo o lo promuevan y a facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de la normativa.

Conforme a los requisitos establecidos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y los artículos 71 y ss. del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre (en adelante RLOPD), la UNED pretende disponer de un Código Tipo que establezca la regulación de la Universidad en materia de seguridad respecto a la totalidad de los tratamientos de datos de carácter personal de los que es titular, el régimen de funcionamiento, los procedimientos aplicables, las obligaciones de los usuarios del Sistema de Información implicados en el tratamiento y uso de la información de carácter personal, así como las garantías de cumplimiento conforme a los principios que rigen la LOPD y el RLOPD.

Debemos tener en cuenta que el Código Tipo tiene carácter deontológico o de buena práctica profesional. Por ello, una vez aprobado por el Consejo de Gobierno de la Universidad, deberá ser notificado a la Agencia Española de Protección de Datos (en adelante AEPD), para ser finalmente depositado e inscrito en el Registro General de Protección de Datos.

Las sugerencias de la AEPD o las actualizaciones meramente formales, en su caso, podrán ser aprobadas por el Comité de Seguridad de la Información.

El Código Tipo deberá estar redactado en términos claros y accesibles y deberá desarrollar, como mínimo los aspectos que se relacionan a continuación:

- La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
- Las previsiones específicas para la aplicación de los principios de protección de datos.
- El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición a sus datos personales.
- La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.
- Las acciones formativas en materia de protección de datos dirigidas a quienes traten datos de carácter personal, especialmente en cuanto a su relación con los afectados.
- Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento de lo establecido en el Código Tipo.

En particular deberá contenerse en el Código:

- Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.
- Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.
- Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición a sus datos personales.
- Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

## **2. CONTENIDO DEL CÓDIGO TIPO**

### **2.1. MARCO NORMATIVO**

- Constitución Española. Art. 18.4
- Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, aplicable a partir del 25 de mayo de 2018.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)
- 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 (RLOPD)
- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades modificada por Ley Orgánica 4/2007, de 12 de abril:
  - Artículo 57
  - Artículo 62
  - Disposición adicional 21
- Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público
  - Artículo 333
  - Disposición adicional vigésima sexta
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por el R.D. 951/2015, de 23 de octubre
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras
- Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos relativa al ejercicio de los derechos de acceso, rectificación y cancelación
- Real Decreto 1239/2011, de 8 de septiembre, por el que se aprueban los Estatutos de la UNED
- Política de Seguridad de la Información de la UNED, aprobada en Consejo de Gobierno de 13 de diciembre de 2016
- Normativa de Seguridad y buen uso del Sistema de Información de la UNED, aprobada en Consejo de Gobierno de 3 de marzo de 2015, modificada el 26 de abril de 2016

## 2.2. DEFINICIONES

- **Datos personales:** toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de

localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- **Tratamiento:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **Elaboración de perfiles:** toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona.
- **Seudonimización:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- **Fichero:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Responsable del tratamiento o responsable:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.
- **Encargado del tratamiento o encargado:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- **Destinatario:** la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.
- **Tercero:** persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo autoridad directa del responsable o del encargado.
- **Consentimiento del interesado:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- **Violación de la seguridad de los datos personales:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

- **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

### **2.3. ÁMBITO DE APLICACIÓN**

La UNED tiene entre sus objetivos garantizar la protección de los datos de carácter personal de todas aquellas personas que con ella se relacionan: estudiantes, profesores, personal de administración y servicios y, en general, cualquier otro ciudadano que en algún momento de su vida tenga relación con nuestra institución.

La UNED aplicará lo dispuesto en este Código al Rectorado, Facultades, Escuelas Universitarias y a las Bibliotecas adheridas a este ámbito de aplicación.

Este Código de buenas prácticas será aplicable a todo tratamiento de datos de carácter personal titularidad de la UNED, con independencia del soporte en el que se encuentren (manual, automatizado o mixto).

Todos los usuarios del Sistema de Información de la UNED, así como Encargados de Tratamiento, quedarán obligados a cumplir las disposiciones contenidas en este texto.

### **2.4. ENTRADA EN VIGOR**

El presente Código Tipo entrará en vigor y será plenamente eficaz a partir de la fecha de su inscripción en el Registro General de la Agencia de Protección de Datos.

El presente Código tiene una duración indefinida, si bien por la propia naturaleza de las exigencias contenidas en el mismo, podrá ser modificado para su actualización. Los cambios a introducir en tales situaciones serán elaborados por el Departamento de Política Jurídica de Seguridad de la Información en base a las competencias que tiene atribuidas en el presente Código, siendo notificados previamente a la Agencia Española de Protección de Datos para su aprobación.

Igualmente, se pondrá en conocimiento de los usuarios del Sistema de Información de la UNED, toda modificación del presente Código Tipo, el cual se entenderá aceptado y asumido por la Entidad si en el plazo de 10 días desde su recepción no manifiesta su voluntad contraria al mismo.

### **2.5. OBLIGACIONES POSTERIORES A LA INSCRIPCIÓN DEL CÓDIGO TIPO**

De conformidad con lo dispuesto en el artículo 78 del RLOPD, la UNED como entidad promotora del presente Código Tipo, una vez que el mismo haya sido publicado, asumirá las siguientes obligaciones:

- Mantener accesible al público, a través de su Portal de Transparencia y el espacio WEB de la UNED de Protección de Datos, la información actualizada sobre el contenido del Código Tipo, los procedimientos de adhesión, en su caso, y de garantía de su cumplimiento y la relación de adheridos, si los hubiera, a la que se refiere el art. 77 del RLOPD. Esta información se presentará de forma concisa, clara y estará permanentemente accesible por medios electrónicos.
- Remitir a la Agencia Española de Protección de Datos una Memoria anual sobre las actividades realizadas para difundir el Código Tipo, promover la adhesión a éste, las actuaciones de verificación del cumplimiento del Código y sus resultados, las quejas, reclamaciones tramitadas, el curso que se les hubiera dado y cualquier otro aspecto que la UNED considerase adecuado destacar.
- Evaluar periódicamente la eficacia del Código Tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general de protección de datos existente en cada momento.

Esta evaluación se llevará a cabo, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del Código a la modificación de la normativa aplicable en un plazo inferior.

## **2.6. PRINCIPIOS DE LA PROTECCIÓN DE DATOS**

Los principios de la protección de datos constituyen la base mediante la cual se articula el derecho fundamental a la protección de datos. Son de obligado cumplimiento desde el momento en que se produce la recogida de los datos de un interesado o afectado (persona titular de los datos), siempre y cuando dichos datos sean almacenados en un fichero, ya sea total o parcialmente automatizado, o en papel.

Dado el carácter obligatorio, tanto los usuarios del Sistema de Información como, en su caso, quien se encargue del tratamiento deben adoptar las medidas necesarias para que no sean vulnerados. El incumplimiento puede suponer una lesión del derecho fundamental a la protección de datos de carácter personal.

### **2.6.1. Calidad de los datos**

El principio de calidad de los datos establece una serie de fundamentos, por los que deben ser recogidos y tratados los datos personales.

**Licitud en la recogida de datos.-** Está prohibida la recogida de datos por medios fraudulentos o engañosos, que induzcan a error a la persona respecto a la finalidad para la que se recaban los datos.

**Pertinencia, adecuación y finalidad de los datos.-** Los datos personales que se recojan deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que hayan sido obtenidos. Se trata de evitar una recopilación de datos masiva que se aparte de la necesidad y finalidad para la que dichos datos pretendan ser utilizados y tratados.

**Compatibilidad y uso no distinto por el que se facilitaron los datos.-** No podrán utilizarse los datos para finalidades incompatibles o distintas de las inicialmente previstas.

**Especificación y legitimidad de la finalidad.-** La finalidad debe estar expresada (determinada), especificada (explícita) y no ser contraria a la Ley (legítima).

**Veracidad, actualización y exactitud de los datos.-** Los datos deberán ser exactos y mantenerse actualizados, de manera que respondan con veracidad a la situación actual de su titular.

**Limitación temporal en la conservación de los datos.-** Los datos personales sólo deben conservarse durante el tiempo necesario para las finalidades del tratamiento para el que han sido recogidos. Deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes para el fin con el que se obtuvieron.

### **2.6.2. Derecho de información en la recogida de datos**

El derecho de información establece las condiciones en que se deben recoger, tratar y ceder los datos de carácter personal para salvaguardar la intimidad y demás derechos fundamentales.

A través del derecho de información en la recogida de datos, la LOPD establece a la vez un derecho para el ciudadano y un deber para el Responsable del Fichero. Por un lado, el ciudadano tiene derecho a saber quién recoge sus datos, para qué los recoge, quién va a ser en su caso destinatario de esa información, los derechos que le asisten y dónde dirigirse para poder ejercerlos. Y por otro lado, el Responsable del Fichero tiene la obligación de informar al interesado, cuyos datos van a ser tratados, en los términos regulados en el artículo 5 de la LOPD, *de forma previa, expresa, precisa e inequívoca*, acerca de lo siguiente:

- De la incorporación de sus datos a un fichero.
- De la identidad y dirección del Responsable del Fichero o, en su caso, de su representante.
- De la finalidad o uso del fichero.
- De los destinatarios o cesionarios de los datos personales.
- Del carácter obligatorio o facultativo de la respuesta en un cuestionario.

- De las consecuencias, ante la negativa a suministrar los datos personales.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Esta información ha de estar contemplada, de forma suficientemente legible y accesible, en los formularios o cuestionarios, en papel o electrónicos (Internet), que utilicen para recoger los datos.

En el caso de que los datos de carácter personal no hubieran sido recabados o proporcionados directamente por la persona, el Responsable del Fichero o su representante deben informarle de esa recogida dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad.

Si está previsto que los datos sean transmitidos a otras personas, la información debe realizarse antes de la primera cesión o comunicación de los datos.

Este derecho de información es esencial porque condiciona el ejercicio de otros derechos tales como el derecho de acceso, rectificación, cancelación y oposición, expuestos a continuación.

### **2.6.3. Consentimiento del afectado**

Para el tratamiento o, en su caso, cesión o comunicación de datos de carácter personal, como regla general, se deberá recabar el consentimiento inequívoco del afectado o interesado. No obstante, la Ley prevé una serie de excepciones a la obligación de obtener este consentimiento, por parte del titular del fichero:

#### **2.6.3.a) En relación a tratamientos de datos**

- a. Cuando así lo autorice una Ley o una norma de derecho comunitario europeo.
- b. Cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.
- c. Cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- d. Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado.
- e. El consentimiento al tratamiento de los datos podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

#### **2.6.3.b) En relación a cesiones o comunicaciones de datos**

Este apartado se desarrolla en el punto 2.6.7. "Comunicación de datos", de este Código.

### **2.6.3.c) Revocación del consentimiento**

La revocación se ha de poder manifestar a través de un medio sencillo y gratuito.

En particular, no será válido que el Responsable del Fichero o Tratamiento exija para revocar el consentimiento el envío de cartas certificadas o sistemas semejantes, la utilización de servicios de telecomunicaciones que impliquen una tarificación adicional al afectado (como llamadas a números 902 o similares) o cualquier otro medio que implique un coste adicional.

Cuando se revoque el consentimiento, el Responsable del Fichero deberá cesar en el tratamiento de los datos en el plazo máximo de 10 días hábiles desde que recibiera la comunicación.

Asimismo, en aquellos casos en que el Responsable del Fichero hubiese cedido los datos a terceros, deberá comunicarle a éstos, en el plazo de 10 días hábiles, la revocación del consentimiento para que ellos también cesen en el tratamiento de los datos.

### **2.6.4. Principio de seguridad de los datos**

El Responsable del Fichero y, en su caso, a quien éste encargue el tratamiento de los datos, deberán adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales integrados en los ficheros, evitando que éstos puedan perderse, alterarse, usarse o ser accesibles a personas no autorizadas.

Las medidas de seguridad se adoptarán tomando en consideración el 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.

La normativa prevé medidas de seguridad para los ficheros automatizados (informáticos) y no automatizados (en papel), según la naturaleza de los datos personales que contengan.

### **2.6.5. El deber de secreto en el tratamiento de datos**

El Responsable del Fichero y quienes intervengan en cualquier fase del tratamiento de los datos personales, están obligados a guardar secreto profesional respecto de los mismos. Además, existen obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero (Responsable del Fichero).

Teniendo en cuenta estas circunstancias, el Responsable del Fichero no sólo debe preocuparse por respetar su propio deber de secreto, también debe asegurarse de que todo el personal a su servicio mantiene la confidencialidad del tratamiento, para lo cual se deben adoptar, al menos, las siguientes medidas:

- Informar al personal de su deber de secreto.

El Responsable del Fichero deberá asegurarse de que todo el personal a su cargo

(tanto personal interno como usuarios externos, subcontratados), conoce su obligación respecto a los datos personales a los que tenga acceso y las consecuencias de su incumplimiento.

- Adoptar las medidas necesarias para garantizar la confidencialidad de los datos a los que se ha accedido, implantando las medidas técnicas y de carácter organizativo necesarias para impedir que el personal a su servicio pueda revelar datos de carácter personal a terceras personas.

#### **2.6.6. Datos especialmente protegidos**

Los datos especialmente protegidos son aquellos que revelan la ideología, afiliación sindical, religión o creencias de la persona y que sólo con el consentimiento expreso y por escrito puede ser objeto de tratamiento. Esto está relacionado con el mandato constitucional de que nadie puede ser obligado a declarar sobre su ideología, religión o creencias.

Son también datos especialmente protegidos los que hacen referencia al origen racial o étnico, vida sexual y a la salud (se entiende por datos de salud, datos pasados, presentes y futuros, sobre el estado físico o mental de una persona, los datos relativos al grado o porcentaje de su minusvalía, así como información genética).

La UNED tiene declarados ficheros con nivel de seguridad alto, debido a que, principalmente, se recaban datos de salud. Tal es el caso de los ficheros de becas al estudiante, gestión de investigación, prevención de riesgos laborales, igualdad y acción social, estudiantes con discapacidad (UNIDIS) y Servicio de Psicología Aplicada.

No es necesario el consentimiento de la persona cuando el tratamiento de los datos sobre ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual sea preciso para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto.

Tampoco es preciso el consentimiento cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona que esté física o jurídicamente incapacitada para dar su consentimiento.

#### **2.6.7. Comunicación de datos**

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

El consentimiento exigido en el apartado anterior no será preciso, sin perjuicio de lo dispuesto en el artículo 10 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre, en los siguientes supuestos:

- a) Cuando la cesión está autorizada en una Ley.
- b) Cuando se trate de datos recogidos de fuentes accesibles al público.
- c) Cuando 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) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o 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) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

El consentimiento para la comunicación de los datos de carácter personal tiene también carácter revocable.

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.

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

La comunicación de datos o su uso interno con fines de investigación sólo se producirá si está autorizada en una Ley o se ha utilizado un procedimiento de disociación.

### **2.6.7.1. Comunicación de datos personales por parte de la UNED**

La comunicación de datos a terceros sólo se producirá cuando una Ley obligue a la Universidad a esa comunicación o el interesado consienta.

La UNED, en cumplimiento de la legislación vigente, realiza las siguientes comunicaciones para el ejercicio de las funciones que tienen atribuidas y en los supuestos y condiciones establecidos en la normativa correspondiente:

1. Datos de estudiantes:
  - a. Ministerio de Educación Cultura y Deporte
  - b. Universidades colaboradoras
  - c. Hacienda Pública y Administración Tributaria
  - d. Entidades bancarias y Aseguradoras
  - e. Federaciones Deportivas
  - f. Órganos judiciales
  - g. Fuerzas y cuerpos de seguridad del Estado
  - h. Ministerio del Interior y Ministerio de Defensa
  - i. Órganos de la Unión Europea
  - j. Fundación UNED
  
2. Datos de empleados:
  - a. Hacienda Pública y Administración Tributaria
  - b. Tribunal de Cuentas
  - c. Tesorería General de la Seguridad Social
  - d. MUFACE
  - e. Entidades financieras
  - f. Registro Central de Personal (MHFP)
  - g. Sindicatos, Juntas de Personal
  - h. Entidades sanitarias; Servicio de prevención
  - i. Inspección de Trabajo y Seguridad Social

### 3. Datos de investigadores:

- a. Entidades bancarias y Aseguradoras
- b. Ministerio de Economía, Industria y Competitividad
- c. Ministerio de Empleo y Seguridad Social
- d. Ministerio de Sanidad, Servicios Sociales e Igualdad
- e. Instituto de la Mujer
- f. Instituto de Salud Carlos III
- g. Consejería de la Comunidad de Madrid
- h. Junta de Comunidades de Castilla la Mancha

#### **2.6.7.2. Las transferencias internacionales de datos**

No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal con destino a países que no proporcionen un nivel equiparable a la LOPD, salvo que se obtenga autorización previa del/la Director/a de la Agencia Española de Protección de Datos.

Lo dispuesto en el párrafo anterior no será de aplicación si el afectado hubiera dado su consentimiento inequívoco a la transferencia o ésta fuera necesaria para la ejecución de un servicio o contrato en interés del beneficiario o en cualquiera de los supuestos previstos en el artículo 34 de la LOPD.

En la actualidad, únicamente están previstas las transferencias internacionales de datos relacionadas a continuación:

1. Respecto a la información contenida en el fichero CUID a Universidades u otras organizaciones dentro del ámbito académico, recabándose para ello el consentimiento inequívoco, previo, del interesado en cada caso.
2. En el Fichero de Títulos Propios a entidades públicas o privadas de ámbito académico, contando con el consentimiento inequívoco, previo, del interesado en cada caso.
3. Como consecuencia del Informe emitido por la AEPD y el convenio suscrito entre la UNED y Microsoft Ibérica, sobre OFFICE 365, se ha inscrito en la AEPD el fichero “Gestión del correo dominio uned.es en la Nube”, en el que consta la transferencia internacional de datos a Estados Unidos.

#### **2.6.8. Las prestaciones de servicios con y sin acceso a datos de carácter personal**

##### **2.6.8.1. Prestaciones de servicios con acceso a datos**

En el artículo 12 de la LOPD, así como en los art. 20, 21 y 22 del RLOPD, se señalan las condiciones en que se deben recoger, tratar y en su caso ceder los datos de carácter personal para no perjudicar la intimidad y demás derechos fundamentales de los ciudadanos, en

aquellos supuestos en los que un tercero (en adelante, Encargado de Tratamiento), preste un servicio a la UNED que conlleve un acceso a datos de carácter personal titularidad de la Universidad.

- No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio a la UNED.
- La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones de la UNED, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el caso de incumplimiento de las estipulaciones establecidas, el encargado del tratamiento será considerado, también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. En el contrato se estipularán, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.
- Si el encargado de tratamiento necesita para la prestación de un servicio a la UNED subcontratar con un tercero parte del tratamiento deberá contar con autorización previa escrita de la Universidad. Esta autorización puede estar contemplada en el contrato del servicio con el encargado de tratamiento o ser formalizada posteriormente pero siempre antes de realizar la subcontratación. En cualquier caso, el subcontratista tendrá las obligaciones de encargado de tratamiento y seguirá las instrucciones de la UNED para ese tratamiento así como el cumplimiento de las disposiciones legales correspondientes.
- Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos a la UNED, 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.
- En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

#### **2.6.8.2. Prestaciones de servicios sin acceso a datos**

De conformidad con el art. 83 del RLOPD, el Responsable del Fichero adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, 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 personales.

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

## **2.7. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN**

### **2.7.1. Aspectos comunes**

Junto a los anteriores principios rectores del tratamiento de datos de carácter personal, la normativa reconoce, de forma expresa, a la persona los derechos de acceso, rectificación, cancelación y oposición (en adelante, ARCO) y que atienden a las siguientes características y reglas para ser ejercitados por la persona.

Los derechos ARCO son personalísimos, por lo que sólo pueden ser ejercidos por la propia persona, titular de los datos.

En todo caso, cualquier persona puede ejercitar los derechos ARCO a través de representante voluntario, esto es, persona que libremente se elija para que actúe, en su nombre y representación. No es preciso que la autorización o los poderes otorgados consten en escritura pública formalizada ante Notario. No se admite el apoderamiento verbal.

Son derechos independientes, por lo que no hay que ejercitar uno para poder ejercitar después otro. Por ejemplo, el derecho de acceso no ha de ejercitarse necesariamente de forma previa a la solicitud de rectificación o cancelación de datos personales, aunque ayude a constatar un tratamiento de datos erróneo o que no deberían ser tratados.

El titular del fichero (Responsable del Fichero) debe proporcionar medios sencillos y gratuitos para que la persona pueda ejercitar estos derechos.

Cuando el titular del fichero (Responsable del Fichero) tenga servicios de atención al cliente o para formular reclamaciones, el afectado podrá ejercer sus derechos ARCO a través de tales servicios. En estos supuestos, para acreditar la identidad de quien ejercita los derechos podrán usarse los mismos mecanismos que se empleen por el Responsable para identificar a los clientes en la prestación de servicios o en la contratación de productos.

El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud de ejercicio de los derechos ARCO.

La solicitud o petición de ejercicio de derechos ha de contener la siguiente información y documentación:

- Nombre y apellidos del interesado.
- Fotocopia de su DNI, 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 persona eximirá de la presentación de las fotocopias del DNI o documento equivalente.

- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones.
- Fecha y firma del solicitante.
- En su caso, documentos acreditativos de la petición que formula.

Además, la persona tiene derecho a que su solicitud sea contestada por el titular del fichero (Responsable del Fichero), incluso en el supuesto en que sus datos no figuren en los ficheros de dicho Responsable. En tal caso, el Responsable de fichero o Tratamiento deberá informar de la ausencia de datos en su fichero.

Si la solicitud no reuniese los requisitos necesarios, el afectado tiene derecho a que el titular del fichero (Responsable del Fichero o Tratamiento) le solicitase su subsanación.

### **2.7.2. El derecho de acceso**

Es el derecho que se reconoce a la persona para ser informada sobre qué datos de carácter personal suyos están sometidos a tratamiento, de dónde han obtenido sus datos, para qué finalidades o usos concretos tratan sus datos y de las cesiones o comunicaciones de sus datos se hayan hecho o que se prevean realizar.

El derecho de acceso es independiente del que otorgan a las personas otras leyes y, en particular, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (derecho de acceso a expedientes administrativos).

Al ejercitar el derecho de acceso, la persona podrá elegir cómo recibir o acceder a la información, a través de uno o varios de los siguientes medios:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo, certificado o no.
- Telecopia.
- Correo electrónico u otros sistemas de comunicaciones electrónicas.
- Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el Responsable de Fichero o Tratamiento

La información que se proporcione, cualquiera que sea el soporte en que fuera facilitada, deberá ser legible e inteligible, sin que haya de utilizarse claves o códigos para acceder a la misma.

El Responsable del Fichero o Tratamiento deberá resolver sobre lo solicitado en el plazo de un mes desde la recepción de la solicitud. También deberá hacerlo aunque no disponga de datos del afectado. Si transcurrido dicho plazo, la solicitud no ha sido atendida adecuadamente, el interesado podrá dirigirse a la Agencia Española de Protección de Datos con copia de la solicitud cursada y de la contestación recibida (si existiera), para que ésta a su vez se dirija a la oficina designada con el objetivo de hacer efectivo el ejercicio de ese derecho.

Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que está obligado, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

Este derecho sólo podrá ser ejercido en intervalos superiores a 12 meses. Hasta que no transcurra este plazo de tiempo no podrá volver a ejercitarse. Excepcionalmente, podrá ejercitarse antes de finalizar el plazo, cuando la persona acredite tener un interés legítimo.

### **2.7.3. El derecho de rectificación**

Es el derecho que se reconoce a la persona para solicitar la rectificación de sus datos de carácter personal cuando encuentre que son inexactos o incompletos.

En la solicitud de rectificación deberá indicar los datos que son erróneos y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada.

El Responsable del Fichero o Tratamiento tiene el deber de atender la solicitud del derecho de rectificación en el plazo máximo de 10 días hábiles a contar desde su recepción.

Si los datos rectificadas hubieran sido cedidos previamente a un tercero, el Responsable de Fichero deberá notificar la rectificación practicada a este cesionario.

### **2.7.4. Derecho de cancelación**

Es el derecho que se reconoce a la persona para solicitar la cancelación de sus datos de carácter personal cuando encuentre que son inadecuados, excesivos o su tratamiento no se ajusta a la Ley.

No obstante, la cancelación dará lugar al bloqueo de datos cuando sea preciso conservar éstos únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, de cara a posibles responsabilidades.

El bloqueo tendrá una duración equivalente al plazo de prescripción de dichas responsabilidades, debiéndose proceder a la total supresión de los datos una vez cumplido el mismo.

El Responsable del Fichero o Tratamiento tiene el deber de atender la solicitud del derecho de cancelación en el plazo máximo de 10 días hábiles a contar desde su recepción.

### **2.7.5. Derecho de oposición**

Es el derecho que se reconoce a la persona para oponerse a que se traten sus datos de carácter personal o se cese en el tratamiento de los mismos, en los siguientes supuestos:

- Cuando no sea necesario su consentimiento para poder tratar sus datos, como consecuencia de la existencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.
- Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.
- Cuando el tratamiento tenga por finalidad adoptar una decisión referida al afectado y basada únicamente en un tratamiento automatizado (informático) de sus datos de carácter personal.

El afectado debe dirigir al Responsable del Fichero o Tratamiento la solicitud ejercitando tal derecho. Cuando la oposición al tratamiento se base en la primera de las causas descritas, el afectado deberá indicar los motivos que justifican el ejercicio de tal derecho.

El Responsable del Fichero o Tratamiento tiene el deber de atender la solicitud del derecho de oposición en el plazo máximo de 10 días hábiles a contar desde su recepción.

En caso de estimarse procedente la oposición, el Responsable de Fichero deberá excluir del fichero los datos de carácter personal de la persona solicitante.

## **2.8. ACCIONES FORMATIVAS EN MATERIA DE PROTECCIÓN DE DATOS**

La eficacia del Código no se logra con el mero cumplimiento formal de las obligaciones establecidas en la LOPD y en el RLOPD. La eficacia del Código se logrará cuando se alcance un alto nivel de concienciación por parte de los usuarios del Sistema de Información.

Para cumplir dicho objetivo, la UNED informa y asesora a los usuarios de la Universidad y a los Centros Asociados a la UNED, a través del Departamento de Política Jurídica de Seguridad de la Información.

Asimismo, el personal del Departamento y del Centro de Tecnología de la UNED asistirá a reuniones, cursos y jornadas, especialmente de la AEPD, con el fin de conocer y aplicar las novedades legales en materia de protección de datos y de seguridad informática, que dará a conocer a todos los responsables de ficheros o tratamientos.

Igualmente, el Departamento, en el ejercicio de las funciones que tiene atribuidas en este Código Tipo, organizará al menos una vez al año, una jornada, conferencia o curso, al objeto de formar en materia de Protección de Datos al personal y demás usuarios que traten datos de carácter personal titularidad de la Universidad. Como materia complementaria se formará al personal de las distintas unidades en materia de Seguridad informática, seleccionando, para su visualización, videos ilustrativos en esta material. Además, al amparo

del Convenio de Colaboración suscrito entre la UNED y la AEPD de fecha 10 de mayo de 2005, de cooperación educativa, se podrán establecer las acciones formativas mediante prácticas con estudiantes, que se decidan organizar conjuntamente.

## **2.9. GESTIÓN DE LOS FICHEROS DE DATOS DE CARÁCTER PERSONAL**

La LOPD define como Responsable del Fichero a la *“persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”*.

A estos efectos, la UNED se erige como Responsable de todos aquéllos ficheros, con datos de carácter personal, que obran en sus sistemas de información (informático y en papel), y que derivan de la prestación de los servicios atribuidos.

### **2.9.1. Procedimiento interno de detección de ficheros en la UNED**

De conformidad con la normativa en materia de protección de datos, toda persona o entidad que posea ficheros con datos personales está obligada a inscribir en el Registro General de protección de Datos, la estructura de los ficheros de que disponga (artículo 26.1.LOPD).

**Dato de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables.

**Fichero:** Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

La relación de ficheros que contengan datos de carácter personal contemplados en el Registro General de Protección de Datos debe reflejar la realidad de los tratamientos de datos que se llevan a cabo por la Universidad, ya sea en soporte manual o automatizado.

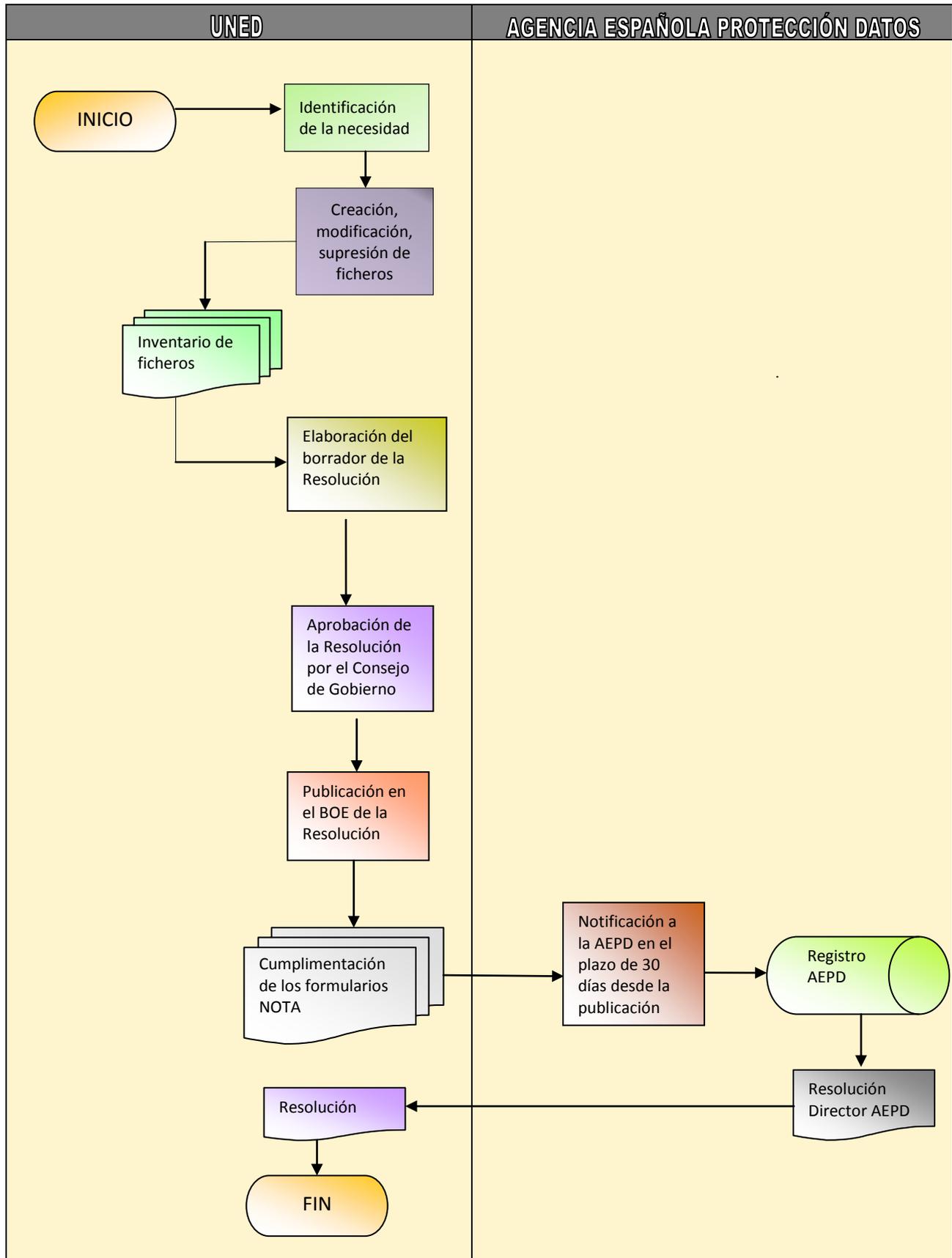
En este sentido, resulta esencial la colaboración de los usuarios y responsables de las Unidades de la UNED en la detección de nuevos tratamientos de datos de carácter personal que puedan llevarse a cabo con el objeto de valorar, si dicho tratamiento de datos podría ser integrado en alguno de los ficheros actualmente declarados o en su caso, proceder a la creación e inscripción de un nuevo fichero.

En la Intranet de la UNED, dentro del Espacio de Protección de Datos, en el menú “Ficheros inscritos”, se encuentran los modelos de solicitudes para comunicar la creación, la modificación o supresión de ficheros de la Universidad.

### **2.9.2. Procedimiento de declaración de ficheros LOPD**

La relación actualizada de ficheros jurídicos que se han creado en la Universidad, y que engloban los diferentes tratamientos de datos de carácter personal inscritos ante el Registro de la Agencia Española de Protección de Datos, está disponible en la página [web de la UNED](#) que, en aras de la seguridad jurídica, se ha dispuesto refundir en un único Texto.

A continuación se muestra el flujograma que concreta los pasos a seguir por la UNED para la declaración de ficheros (inscripción, modificación y, o supresión) ante el Registro de la Agencia Española de Protección de Datos.



## **2.10. MEDIDAS DE SEGURIDAD APLICABLES SOBRE LOS TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL**

### **2.10.1. Medidas de seguridad**

De conformidad con el art. 9 de la LOPD, el Responsable del Fichero, y, en su caso, el Encargado del Tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

La UNED, los usuarios del Sistema de Información y los Encargados de Tratamiento están obligados a implementar las medidas de seguridad que correspondan recogidas en los artículos 89 a 114 del RLOPD.

Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto. Estos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

#### **a) Nivel Básico**

Todo fichero que contenga datos de carácter personal

#### **b) Nivel Medio**

Deberá ser implementado por aquellos ficheros que almacenen:

- Datos relativos a la comisión de infracciones administrativas o penales
- Hacienda pública
- Servicios financieros
- Ficheros de solvencia patrimonial y crédito
- Datos que permitan realizar una evaluación de la personalidad del individuo

#### **c) Nivel Alto**

Cuando el tratamiento contenga datos relativos a:

- Salud
- Ideología
- Afiliación sindical
- Religión
- Creencias
- Origen racial
- Vida sexual
- Datos recabados con fines policiales sin consentimiento de las personas afectadas
- Aquellos que contengan datos derivados de actos de violencia de género

### 2.10.2. Auditorías de cumplimiento

De conformidad con los artículos 96 y 110 del RLOPD, *a partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.*

*Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.*

De este modo, serán objeto de Auditoría los ficheros con medidas de seguridad, técnicas y organizativas, de nivel Medio o Alto.

La realización de las auditorías preceptivas con carácter bienal, permiten verificar la correcta aplicación de las medidas de seguridad exigidas por la normativa, así como las directrices y obligaciones incluidas en el presente Código.

Una vez realizada la auditoría por parte de la entidad externa contratada al efecto por parte de la UNED, se elabora un Informe de Auditoría, que contiene:

- El resultado del análisis efectuado.
- Las deficiencias que, en su caso, fuesen encontradas y propuesta de medidas correctoras o complementarias.
- Recomendaciones que, en su caso, se pudieren efectuar.
- Opinión o conclusiones de los auditores acerca del grado de cumplimiento de la normativa legal.

Estos Informes estarán a disposición de la Agencia Española de Protección de Datos y contendrán las medidas de seguridad, técnicas y organizativas de nivel medio y alto, que se deben adoptar en los ficheros titularidad de la UNED.

La metodología utilizada para la realización de las Auditorías comprende, entre otros, la realización de entrevistas, inspección visual, análisis de la documentación y comprobación y verificación de la documentación requerida por parte del equipo auditor.

Los informes quedan a disposición de los Responsables de Seguridad, a los efectos de elevar las conclusiones a los Responsables de Ficheros para que se adopten las medidas correctoras adecuadas.

### 2.10.3. Ficheros temporales

En el trabajo diario es habitual la generación de ficheros temporales por parte de los usuarios para atender a distintas necesidades, es decir, ficheros obtenidos a partir de un fichero matriz o principal y que se crean, normalmente, en un procesador de texto (Microsoft Word) o en una hoja de cálculo (Microsoft Excel).

Los ficheros temporales adoptarán las medidas de seguridad exigidas por el RLOPD. Por otro lado, la utilización de estos ficheros requiere el cumplimiento de uno de los Principios de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), el de la calidad de los datos. En este sentido el art.4.3 señala que: *“los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado”*.

De no cumplir con este principio, estaríamos ante una infracción grave según el art.44.3 c) de la citada Ley.

Por ello, todo fichero temporal o copia de trabajo será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación. Al respecto, en la Normativa de seguridad y buen uso del Sistema de Información de la UNED se establece que transcurrido un mes, si el usuario detecta la necesidad de continuar utilizando la información almacenada en el fichero, deberá comunicárselo al Responsable de seguridad, para adoptar sobre el mismo las medidas oportunas.

### 2.10.4. El documento de seguridad

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 el RLOPD.
- c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
- f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

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

En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en el Título VIII del RLOPD, el documento de seguridad deberá contener además:

- a) La identificación del responsable o responsables de seguridad.
- b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

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.

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.

### 2.11. ROLES Y RESPONSABILIDADES

**El Responsable de Seguridad de la UNED:** Es la persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. Es el encargado de autorizar, coordinar, controlar y en algunos supuestos ejecutar las medidas definidas en el documento seguridad.

En la UNED han sido designados los siguientes responsables de seguridad:

**Para ficheros automatizados:** El Director del Centro de Tecnología de la UNED

**Para ficheros no automatizados:** La Jefa de Sección de Protección de Datos

**El Gestor de Fichero:** Es la figura intermedia entre el Responsable del Fichero y los usuarios del tratamiento de los datos personales, en la que se delega ciertas actividades de control y ejecución de medidas en aras a colaborar con las obligaciones del Responsable de Seguridad y existir un mayor acercamiento con los usuarios de cada fichero en el cumplimiento de sus funciones en esta materia.

### **Comité de Seguridad de la Información de la UNED**

Se crea el Comité de Seguridad de la Información de la UNED, por resolución rectoral de 29 de abril de 2014, como órgano colegiado de la Universidad.

Se encargará de coordinar y centralizar la gestión tecnológica en materia de seguridad, que será competencia de la Gerencia y del Centro de Tecnología de la UNED (CTU).

Está formado por los siguientes miembros:

- Presidente: El Gerente, como Responsable de la Información
- Vocales:
  - El Vicerrector de Medios y Tecnología, como Responsable de Seguridad de la Información
  - El Vicegerente de RR.HH. y organización, como Responsable del Servicio
  - El Responsable del Sistema
  - El Director del CTU
  - La Secretaria General
  - La Jefa de Departamento de Política Jurídica de Seguridad de la Información
  - El Administrador de la Seguridad del Sistema
  - El Asesor de Seguridad
  - La Jefa de Sección de Protección de Datos y Secretaria del Comité

### **El Delegado de protección de datos de la UNED**

Esta figura, de nueva creación por el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, será designada atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos específicos especializados en Derecho, la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en esta materia.

#### **2.12. LA COMISIÓN DE CONTROL DEL CÓDIGO TIPO**

Se constituye una **Comisión de Control del Código Tipo** en la UNED integrada por las siguientes personas:

- El Gerente, actuando como Presidente de la Comisión
- Los Responsables de Seguridad en materia de protección de datos
- El Vicegerente de RR.HH. y organización
- El Asesor en materia de seguridad, actuando como Secretario
- El Delegado de protección de datos

Los miembros de la Comisión de Control deberán tener formación en materia de protección de datos.

Las funciones de la Comisión son las siguientes:

1. Representar al Código Tipo ante la Agencia Española de Protección de Datos, atendiendo a las solicitudes de información que existan en su caso y manteniéndola informada respecto a las actuaciones llevadas a cabo.
2. Atender las quejas y reclamaciones que en su caso sean presentadas frente a eventuales incumplimientos del Código.
3. Adoptar todas las medidas que considere necesarias con el objeto de concienciar y formar a los diferentes actores intervinientes en el tratamiento de los datos de carácter personal.
4. Dictar las instrucciones o circulares pertinentes sobre interpretación de las normas del Código Tipo, previa consulta, en su caso, a la Agencia de Española de Protección de Datos.
5. Acordar la remisión de las denuncias recibidas, que puedan ser objeto de la apertura de un expediente disciplinario o una información reservada, al Servicio de Inspección de esta Universidad.
6. Cualquier otra que sea necesaria y pertinente para el correcto desarrollo del Código Tipo.

Funcionamiento de la Comisión

1. La Comisión se reunirá tantas veces como lo considere necesario su Presidente y, en cualquier caso, una vez cada semestre.
2. De las reuniones de la Comisión se levantará acta que será firmada por el Presidente y el Secretario, y se habilitará un libro de actas donde éstas quedarán registradas.
3. En todo caso, la Comisión de Control actuará con plena independencia e imparcialidad.

### **2.13. PRESENTACIÓN DE SUGERENCIAS, QUEJAS O RECLAMACIONES**

Toda persona tendrá derecho a presentar una sugerencia, queja o reclamación cuando tenga constancia de una actuación que contravenga lo dispuesto en la LOPD o en el presente Código Tipo. Esta vía es siempre opcional, sin perjuicio de los derechos de cualquier persona a ser tutelada por la Agencia Española de Protección de Datos, pudiendo el interesado o afectado acudir directamente a la Agencia Española de Protección de Datos para presentar una reclamación ante el incumplimiento de la Ley Orgánica de Protección de Datos.

En el ANEXO 8.1 se recoge un posible modelo de formulario que, en su caso, podrá utilizar la persona que ejercite el derecho a presentar sugerencias, quejas o reclamaciones ante la Comisión de Control del Código Tipo de la UNED.

Este derecho se ejercerá mediante la remisión del escrito a la Comisión de control del Código Tipo, de tal forma que permita tener constancia de su fecha y de su recepción.

Siempre que se presente conforme a lo establecido en los párrafos anteriores, la Comisión de Control dispondrá del plazo de cinco días hábiles, a partir de la notificación de la misma, para comunicar, en su caso, al Responsable del Fichero la sugerencia, queja o reclamación recibida y requerirle la modificación de su actuación, quien, a su vez, dispondrá de un plazo de diez días hábiles para su subsanación.

Todo lo anteriormente señalado, se establece sin perjuicio de la potestad sancionadora que la LOPD atribuye a la Agencia Española de Protección de Datos.

#### **2.14. INFRACCIONES Y SANCIONES**

El régimen sancionador regulado en el presente Código Tipo, se establece sin perjuicio de la potestad sancionadora que la Ley Orgánica 15/1999 y sus disposiciones de desarrollo y concordantes, atribuyen a la Agencia Española de Protección de Datos.

##### **Infracciones leves**

1. El retraso injustificado de la Universidad en la contestación a las solicitudes de ejercicios de los derechos ARCO (acceso, rectificación, cancelación y oposición) que en su caso hayan sido presentadas, así como a las sugerencias, quejas o reclamaciones.
2. No atender los requerimientos de información de la Comisión.
3. Incumplir las obligaciones establecidas en el Código Tipo, cuando no supongan infracciones de la LOPD.

##### **Infracciones Graves**

1. Comisión de dos infracciones leves en el plazo de un año natural.
2. Incumplimiento de las obligaciones establecidas por la LOPD y el RLOPD.
3. No realización de la auditoría RLOPD.
4. Poner trabas en la ejecución de la auditoría RLOPD por parte de la Comisión.

##### **Infracciones Muy Graves**

1. Utilización de los datos para un fin distinto de los reflejados en el presente Código.
2. La reiteración en la comisión de dos infracciones graves.

### **2.15. PROCEDIMIENTO SANCIONADOR**

El procedimiento sancionador se ajustará a lo dispuesto en el Reglamento del Servicio de Inspección de la Universidad, aprobado por el Consejo de Gobierno el 7 de marzo de 2011 y su modificación. (Anexo 4.9)

Asimismo, en el régimen sancionador se tendrá en cuenta lo previsto en la siguiente normativa:

- El Real Decreto 898/1998, de 30 de abril, sobre el Régimen del Profesorado.
- El Real Decreto 33/86, de 10 de enero, por el que se aprueba el Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado.
- El Real Decreto 5/2015, de 30 de octubre, Texto Refundido de la Ley del Estatuto Básico del Empleado Público.
- III Convenio Colectivo de PAS laboral de la UNED. Resolución de 5 de mayo de 2009.
- El Real Decreto de 8 de septiembre de 1954, por el que se aprueba el Reglamento de Disciplina Académica.
- Los Estatutos de la UNED, aprobados por el Real Decreto 1239/2011, de 8 de septiembre, donde se hace referencia en su artículo 212 al Servicio de Inspección, el cual contribuirá al mejor funcionamiento de todos sus servicios y asumir la instrucción de todos los expedientes disciplinarios y para el seguimiento y control general de la disciplina académica. En este sentido el artículo 3 del Reglamento del Servicio de Inspección regula las funciones, donde expresamente se establece que:

*“El Servicio de Inspección ejercerá las siguientes funciones, a instancia del Rector, o, en su caso, de los órganos competentes, según el plan de adecuación aprobado:*

- 1. Velar por el correcto funcionamiento y la calidad de los servicios de la Universidad.*
- 2. La instrucción de todos los expedientes disciplinarios que se incoen a cualquiera de los miembros de la comunidad universitaria.”*

### **2.16. DIFUSIÓN Y EVALUACIÓN DE LA SATISFACCIÓN**

1. De forma complementaria a la difusión del Código Tipo, se ha habilitado la dirección de Internet [PROTECCIÓN DE DATOS UNED](#) donde aparece toda la información considerada de interés en materia de protección de datos en la Universidad.

2. Con objeto de facilitar la recepción de sugerencias, quejas o reclamaciones, relativas a la aplicación de este Código se habilitará un modelo de formulario electrónico para la recogida de esta información en la dirección de Internet [PROTECCIÓN DE DATOS. CÓDIGO TIPO](#) incluido, asimismo, en el ANEXO 8.1. del presente Código Tipo.
3. De forma periódica, y en el medio que se considere más adecuado, se realizará una encuesta de satisfacción sobre la aplicación de los principios de protección de datos de carácter personal en la universidad y, en especial, de este Código Tipo.(ANEXO 9)

#### **2.17. MEMORIA DE ACTIVIDADES**

1. Se realizará una memoria anual sobre las actividades relacionadas con la aplicación de este Código reflejando, entre otros aspectos, las sugerencias, quejas o reclamaciones, así como las felicitaciones recibidas.
2. Esta memoria de actividades será remitida a la Agencia Española de Protección de Datos.

## **ANEXOS**

### **1. DERECHOS ARCO**

- 1.1. PROCEDIMIENTO DE LOS DERECHOS ARCO
- 1.2. FLUJOGRAMA DEL DERECHO DE ACCESO
- 1.3. FLUJOGRAMA DE LOS DERECHOS DE RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN
- 1.4. RESPONSABLES DE DERECHOS ARCO EN LA UNED
- 1.5. SOLICITUDES DE EJERCICIO DE LOS DERECHOS ARCO
  - 1.5.1. Ejercicio de Acceso
  - 1.5.2. Ejercicio de Rectificación
  - 1.5.3. Ejercicio de Cancelación
  - 1.5.4. Ejercicio de Oposición

### **2. CUMPLIMIENTO DEL DEBER DE INFORMACIÓN**

- 2.1. CLÁUSULA INFORMATIVA (art.5. LOPD)
- 2.2. CLÁUSULA MATRÍCULA
- 2.3. CLÁUSULA CARTA DE PAGO MATRÍCULA
- 2.4. CLÁUSULA CEMAV. CONSENTIMIENTO VOZ E IMAGEN
- 2.5. CLÁUSULA CEMAV GRABACIONES
- 2.6. CLÁUSULA CEMAV. RADIO Y TV
- 2.7. CLÁUSULA CONTROL ACCESOS
- 2.8. CLÁUSULA PERSONAL
- 2.9. CLÁUSULA CONVENIOS
- 2.10. CLÁUSULA CURRICULUM VITAE
- 2.11. CLÁUSULA GRABACIONES AULAS AVIP
- 2.12. CLÁUSULA CORREO ELECTRÓNICO
- 2.13. CLÁUSULA PRÁCTICAS FORMATIVAS
- 2.14. CLÁUSULA VIDEO VIGILANCIA
- 2.15. TEXTO INFORMATIVO SOBRE LOS FICHEROS TEMPORALES

2.16. CLÁUSULA DE CONSENTIMIENTO TRANSFERENCIAS INTERNACIONALES DE DATOS

2.17. AVISO LEGAL

2.18. POLÍTICA DE PRIVACIDAD

2.19. PERFIL DEL CONTRATANTE

### **3. FORMACIÓN**

3.1. CURSOS IMPARTIDOS EN LA UNED SOBRE PROTECCIÓN DE DATOS

3.2. CURSOS AL PAS DE FORMACIÓN GENERAL EN PROTECCIÓN DE DATOS

### **4. NORMATIVAS Y PROTOCOLOS**

4.1. REGLAMENTO SOBRE SEGURIDAD Y BUEN USO DEL SISTEMA DE INFORMACIÓN DE LA UNED, aprobado en Consejo de Gobierno el 12 de diciembre de 2017

4.2. NORMATIVA DEL USO DEL CORREO ELECTRÓNICO, aprobada por el Comité de Seguridad de la Información el 22 de noviembre de 2016

4.3. PROCEDIMIENTO DE DESECHADO Y DESTRUCCIÓN DE DOCUMENTOS CON DATOS DE CARÁCTER PERSONAL EN PAPEL, aprobado por el Comité de Seguridad de la Información el 22 de noviembre de 2016

4.4. PROCEDIMIENTO PARA DAR DE BAJA DISPOSITIVOS HARDWARE, aprobado por el Comité de Seguridad de la Información el 22 de noviembre de 2016

4.5. PROCEDIMIENTO DE ACTUACIÓN ANTE LA BAJA DEFINITIVA DEL USUARIO DEL SISTEMA DE INFORMACIÓN DE LA UNED, aprobado por el Comité de Seguridad de la Información el 19 de mayo de 2015

4.6. PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS EN FICHEROS AUTOMATIZADOS

4.7. PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS EN FICHEROS NO AUTOMATIZADOS O EN PAPEL

4.8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNED, aprobada por el Consejo de Gobierno el 13 de diciembre de 2016

4.9. REGLAMENTO DEL SERVICIO DE INSPECCIÓN DE LA UNIVERSIDAD aprobado por el Consejo de Gobierno el 7 de marzo de 2011 y su modificación

### **5. ENCARGADOS DE TRATAMIENTO**

5.1. CLÁUSULA ENCARGADO DE TRATAMIENTO **CON** ACCESO A DATOS

5.2. CLÁUSULA ENCARGADO DE TRATAMIENTO **SIN** ACCESO A DATOS (art. 83 RLOPD)

### **6. FICHEROS**

6.1. ACTUALIZACIÓN, SEMESTRAL, DE LAS ACTIVIDADES Y TRATAMIENTO DE LOS DATOS EN LAS DISTINTAS UNIDADES DE LA UNIVERSIDAD

6.2. SOLICITUD DE CREACIÓN DE FICHERO

6.3. SOLICITUD DE MODIFICACIÓN DE FICHERO

6.4. SOLICITUD DE SUPRESIÓN DE FICHERO

## **7. ROLES Y RESPONSABILIDADES**

7.1. RESOLUCIÓN DEL NOMBRAMIENTO DE LOS MIEMBROS DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

7.2. RESOLUCIÓN DEL NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS DE DATOS DE CARÁCTER PERSONAL

## **8. SUGERENCIAS, QUEJAS O RECLAMACIONES**

8.1. MODELO DE FORMULARIO DE PRESENTACIÓN

## **9. ENCUESTA DE SATISFACCIÓN**

## **10. COMUNICACIONES AL PERSONAL DE LA UNED**

10.1. DÍA DE PROTECCIÓN DE DATOS EN EUROPA

10.2. COMUNICADO SOBRE DESECHADO DE DOCUMENTOS EN PAPEL



## **ANEXO 1.1.**

# **Procedimiento para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de la UNED**

**Departamento de Política Jurídica  
de Seguridad de la Información**

## ÍNDICE

INTRODUCCIÓN.....	3
1. OBJETO.....	4
2. NORMATIVA.....	4
3. FUNCIONES Y RESPONSABILIDADES EN LA UNED.....	4
4. NATURALEZA DE LOS DERECHOS ARCO Y ACCESO A LOS FORMULARIOS.....	5
5. MEDIOS DE PRESENTACIÓN DE LAS SOLICITUDES.....	6
6. ACTUACIONES ANTE LA SOLICITUD DEL EJERCICIO DE LOS DERECHOS ARCO .....	6
7. DEFINICIONES.....	8

## INTRODUCCIÓN

El derecho fundamental a la protección de datos personales deriva directamente de la Constitución. Atribuye a los ciudadanos la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos.

La Constitución Española en su artículo 10 reconoce el derecho a la dignidad de la persona. Por su parte, el artículo 18.4 dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

De ambos preceptos deriva el derecho fundamental a la protección de datos de carácter personal, que ha sido definido como autónomo e independiente por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

En desarrollo del citado artículo 18.4, fue aprobada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

En este sentido la **UNED**:

**INFORMA** sobre el derecho fundamental a la protección de datos regulado en la LOPD.

**AYUDA** a la comunidad universitaria y a los ciudadanos a ejercitar sus derechos y a los responsables y encargados de tratamientos a cumplir las obligaciones que establece la LOPD.

**GARANTIZA** el derecho a la protección de datos en los temas establecidos en la legislación vigente.

El titular de los datos **puede ejercitar los derechos de acceso, rectificación, cancelación y oposición ante el responsable del fichero o tratamiento, gratuitamente**, con el fin de conocer sus datos personales, para solicitar que sean modificados o cancelados, o bien para oponerse a su tratamiento.

De acuerdo con el artículo 23 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre, los derechos de acceso, rectificación, cancelación y oposición tienen **carácter personalísimo**, por lo que deberán ser ejercidos por el mismo interesado.

No obstante, deberán ser ejercitados por el representante legal, cuando el titular sea un menor de edad (a estos efectos, menor de 14 años) o se encuentre en situación de incapacidad.

Todos estos derechos tienen **carácter gratuito** y deben ser respetados por los responsables de los tratamientos de datos personales.

## 1. OBJETO

El objeto de este documento es establecer el procedimiento para la tramitación de las solicitudes del ejercicio de los derechos de acceso, rectificación, cancelación y en su caso, oposición (derechos ARCO) sobre los datos de carácter personal que figuren en poder de la Universidad.

## 2. NORMATIVA

- [INSTRUCCIÓN 1/1998, de 19 de enero](#), de la Agencia de Protección de Datos relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
- [LEY ORGÁNICA 15/1999, de 13 de diciembre](#), de Protección de Datos de Carácter Personal.
- [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.
- [DIRECTIVA 95/46/CE](#), del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo relativo al tratamiento de datos personales y a la libre circulación de estos datos.

## 3. FUNCIONES Y RESPONSABILIDADES EN LA UNED

### Responsable de Fichero

- Tramitar y resolver las solicitudes enviadas por las personas, cuyos datos se encuentran en los ficheros de la Universidad y que sean de su competencia, respondiendo en los términos establecidos en la Ley.
- Responder cualquier solicitud o petición en este sentido, incluso en el supuesto de que se compruebe que no se tienen datos personales del interesado.

### Gestor de fichero

- Tramitar las solicitudes en caso de ausencia del Responsable del Fichero.

### Departamento de Política Jurídica de Seguridad de la Información

- Registrar las solicitudes en el Documento de Seguridad.
- Solicitar, al titular de los datos, la subsanación de las solicitudes que no reúnan los requisitos que exigen las normas.
- Control y revisión del trámite de la solicitud.

### Usuario encargado del trámite

- Facilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición solicitados por el titular de los datos.

## 4. NATURALEZA DE LOS DERECHOS ARCO Y ACCESO A LOS FORMULARIOS

### DERECHO DE ACCESO

[El derecho de acceso](#) permite al titular de los datos conocer y obtener información sobre sus datos de carácter personal sometidos a tratamiento.

- **Justificación:** no es necesaria, salvo si se ha ejercitado el derecho en los últimos doce meses.
- **Plazos:** El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. El acceso podrá hacerse efectivo durante 10 días hábiles tras la comunicación de la resolución.

#### [Formulario para ejercitar el derecho de ACCESO](#)

### DERECHO DE RECTIFICACIÓN

[El derecho de rectificación](#) permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

- **Justificación:** debe indicarse a qué datos se refiere y la corrección que haya de realizarse aportando documentación.
- **Plazo:** 10 días hábiles.

#### [Formulario para ejercitar el derecho de RECTIFICACIÓN](#)

### DERECHO DE CANCELACIÓN

[El derecho de cancelación](#) permite que se supriman los datos que resulten ser inadecuados o excesivos sin perjuicio del deber de bloqueo recogido en la LOPD.

- **Justificación:** debe indicarse el dato a cancelar y la causa que lo justifica, aportando documentación.
- **Plazo:** 10 días hábiles.

#### [Formulario para ejercitar el derecho de CANCELACIÓN](#)

### DERECHO DE OPOSICIÓN

[El derecho de oposición.](#) En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento.

- **Justificación:** concurrencia de motivos fundados y legítimos relativos a su concreta situación personal.
- **Plazo:** 10 días hábiles.

#### [Formulario para ejercitar el derecho de OPOSICIÓN](#)

## RECLAMACIÓN DE TUTELA DE DERECHOS ANTE LA AEPD

En el caso de que los responsables de ficheros no hayan atendido las solicitudes en los plazos marcados por la ley, la LOPD contempla la posibilidad de que el titular de los datos reclame la asistencia de la Agencia Española de Protección de Datos, para que el ejercicio de sus derechos sea efectivo, mediante la presentación de una [Reclamación de Tutela de Derechos](#).

## DENEGACIÓN

El ejercicio del derecho al **acceso** se podrá denegar cuando ya se haya ejercitado en los 12 meses anteriores a la solicitud, salvo que acredite interés legítimo, y en los supuestos que así lo prevea una ley o una norma de derecho comunitario.

Podrán denegarse los derechos de **rectificación y cancelación** en los supuestos previstos en una ley o una norma de derecho comunitario.

## CÓMPUTO DE PLAZOS

De acuerdo con el artículo 6 del RLOPD, en el caso que se señalen plazos por días, se computarán únicamente los hábiles, excluyendo los sábados. Cuando el plazo sea por meses, se computarán de fecha a fecha.

***Nota:** téngase en cuenta el calendario laboral de la Universidad aprobado para el año en curso, para el cómputo de los plazos en lo referente a los periodos vacacionales del personal.*



## 5. MEDIOS DE PRESENTACIÓN DE LAS SOLICITUDES

### PRESENCIALMENTE:

Cumplimentando los formularios correspondientes en cada caso y presentándolo en cualquier Oficina de asistencia en materia de registros. [Encuentre la oficina + cercana](#)

### POR INTERNET:

Por la [Sede electrónica de la UNED](#), a través del Procedimiento del ejercicio de los derechos ARCO.

## 6. ACTUACIONES ANTE LA SOLICITUD DEL EJERCICIO DE LOS DERECHOS ARCO

El ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al Responsable de Fichero, que contendrá:

- Nombre y apellidos del interesado.
- Fotocopia del documento que acredite la identidad del titular de los datos y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes.

- **La utilización de firma electrónica** identificativa **eximirá** de la presentación de las fotocopias del DNI o documentos equivalentes.
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- En su caso, los documentos acreditativos de la petición que formula.
- En caso de ser ejercitado por representante legal: será necesario que acredite tal condición.
- En caso de ser ejercitado por representante voluntario: aportación de copia de su Documento Nacional de Identidad o documento equivalente y la representación conferida por aquél.

### **6.1. Solicitud realizada por TELÉFONO**

Al tratarse de derechos personalísimos y debido a que este medio no permite acreditar la identidad de la persona, se le informará que debe presentar su petición por los medios establecidos en el punto 5 de este documento.

### **6.2. Solicitud realizada de forma PRESENCIAL**

1. Para que exista constancia de la petición, el interesado deberá cumplimentar la solicitud correspondiente adjuntando fotocopia del documento válido que lo identifique. Así como, si es representante legal o voluntario, los documentos que acrediten tal condición.
2. Toda la documentación deberá presentarla en cualquiera de las Oficinas de asistencia en materia de registros.
3. Las solicitudes serán recibidas en la Sección de Registro General de la Universidad, remitiéndose directamente al Departamento de Política Jurídica de Seguridad de la Información. Éste comprobará que aporta los datos personales necesarios para la tramitación, así como fotocopia de los documentos que acredite la identidad de la persona afectada o, en su caso, del representante.

En el caso de que la solicitud no reúna los requisitos especificados anteriormente, se enviará comunicación, al interesado, solicitando la subsanación de la misma.

4. La solicitud se registrará en el Documento de Seguridad de la universidad conteniendo:
  - Número de registro.
  - Fecha de entrada de la solicitud.
  - Fichero afectado y responsable de su tramitación.
  - Fecha de comunicación al Responsable del fichero.
  - Fecha máxima de contestación del Responsable del fichero.
  - Fecha de notificación al interesado.

5. En el plazo máximo de 48 horas, el Departamento remitirá la solicitud, la documentación pertinente y la información relativa a los plazos límites de respuesta, al Responsable del Fichero correspondiente.
6. El Responsable del Fichero, encargado del trámite, notificará al interesado, dentro del plazo establecido, la resolución de la petición de ejercicio del derecho y enviará copia de la misma al Departamento para su registro en el Documento de Seguridad.

### **6.3. Solicitud realizada a través de la Sede electrónica**

1. El interesado deberá cumplimentar el formulario correspondiente incluido en el Procedimiento del ejercicio de los Derechos ARCO de la Sede electrónica.
2. El acceso a la Sede requiere el uso de un certificado digital para las firmas y comparencias reconocido por cualquiera de las entidades oficiales de certificación nacionales, o del DNI electrónico.
3. Las solicitudes se recibirán en la Unidad tramitadora creada al efecto, Departamento de Política Jurídica de Seguridad de la Información, comprobando que aporta los datos personales necesarios para su tramitación y se registrará en el Documento de Seguridad conteniendo los datos descritos en el punto 6.2.4. de este documento.

En el caso de que la solicitud no reúna los requisitos necesarios, se enviará comunicación, al interesado, solicitando la subsanación de la misma.

4. En el plazo máximo de 48 horas, el Departamento remitirá la solicitud, la documentación pertinente y la información relativa a los plazos límites de respuesta, al Responsable del Fichero correspondiente.
5. El Responsable del Fichero, encargado del trámite, resolverá la solicitud dentro del plazo establecido y elaborará la notificación al interesado, remitiéndola al Departamento, que a través de la Sede, la enviará al interesado.

## **7. DEFINICIONES**

### **Afectado o interesado**

Persona física titular de los datos que sean objeto de tratamiento.

### **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 esfuerzos desproporcionados.

### **Datos de carácter personal**

Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

**Fichero de datos personales**

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.

**Responsable de Fichero o del tratamiento**

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice materialmente.

**Responsable de Seguridad**

Persona o personas a quien el Responsable de Fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

**Gestor de fichero**

Se ubica en una situación intermedia entre el Responsable del fichero y los usuarios del sistema. Se le delegan actividades de control en ficheros “concretos”.

**Tratamiento de datos**

Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

## EJERCICIO DEL DERECHO DE ACCESO<sup>(1)</sup>

### DATOS DEL RESPONSABLE DEL FICHERO

**Código de la unidad tramitadora:** U2800039

Departamento de Política Jurídica de Seguridad de la Información

**Nombre / razón social:** Universidad Nacional de Educación a Distancia (UNED)

**Dirección ante la que se ejercita el derecho de acceso:** Calle Bravo Murillo nº 38. 28015-MADRID

CIF: Q2818016D

[Redacted area containing several empty rectangular boxes for data entry]

Localidad y Provincia

Con DNI nº [Redacted] del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 27 y 28 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma y en consecuencia,

### **SOLICITA,**

Que se le facilite gratuitamente el derecho de acceso a sus datos contenidos en los ficheros titularidad de la UNED en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se me remita por correo la información en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso. Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los usos y finalidades para los que se almacenaron.

En \_\_\_\_\_ a de \_\_\_\_\_ de 20\_\_

Firmado,

<sup>1</sup> Se trata de la petición de información sobre los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Universidad Nacional de Educación a Distancia) que es quien dispone de los datos.

<sup>2</sup> También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero

## Instrucciones para el cumplimiento del formulario

1. Es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad y sea considerado válido en derecho, para que el responsable del fichero pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.
2. El derecho de acceso **no podrá llevarse a cabo en intervalos inferiores a 12 meses**, salvo interés legítimo debidamente justificado.
3. Para que la [Agencia Española de Protección de Datos](#) pueda iniciar el procedimiento de tutela de derechos, resulta necesario que haya transcurrido un mes desde la presentación de la solicitud por la que se ejercita el derecho de acceso, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:
  - La negativa del responsable del fichero a facilitar la información solicitada.
  - Copia sellada por el responsable del fichero del modelo de petición de acceso.
  - Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
  - Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud.

## EJERCICIO DEL DERECHO DE RECTIFICACIÓN <sup>(1)</sup>

### DATOS DEL RESPONSABLE DEL FICHERO

**Código de la unidad tramitadora:** U2800039

Departamento de Política Jurídica de Seguridad de la Información

**Nombre / razón social:** Universidad Nacional de Educación a Distancia (UNED)

**Dirección ante la que se ejercita el derecho de acceso:** C/ Bravo Murillo nº 38. 28015-MADRID

CIF: Q2818016D

### DATOS DEL INTERESADO O REPRESENTANTE LEGAL <sup>(2)</sup>

**Nombre y Apellidos**

**Teléfono**

**Correo electrónico**

**Domicilio**

**C.P.**

**Localidad y Provincia**

Con DNI nº  del que acompaña copia, por medio del presente escrito ejerce el derecho de rectificación sobre los datos anexos, aportando los correspondientes justificantes, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 31 y 32 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma y en consecuencia,

### **SOLICITA,**

Que se proceda a acordar la rectificación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Que en caso de que se acuerde que no procede acceder al derecho, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la LOPD.

En

a

de

de 20

Firmado,

<sup>1</sup> Consiste en la petición dirigida al responsable del fichero (Universidad Nacional de Educación a Distancia) con el fin de que los datos personales respondan con veracidad a la situación actual del afectado.

<sup>2</sup> También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero

## Instrucciones para el cumplimiento del formulario

1. Este modelo se utilizará para el caso de que se deban rectificar datos inexactos o incompletos en un fichero.
2. Para probar el carácter inexacto o incompleto de los datos que figuran en los ficheros resulta necesaria la aportación de la documentación que lo acredite al responsable del fichero.
3. Debido al carácter personalísimo de los datos de carácter personal, es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad del afectado y sea considerado válido en derecho, de modo que el responsable del fichero pueda constatarla. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.
4. La rectificación de los datos es **gratuita**.
5. Para que la [Agencia Española de Protección de Datos](#) pueda iniciar el procedimiento de tutela de derechos, resulta necesario que hayan transcurrido diez días hábiles desde la presentación de la solicitud por la que se ejercita el derecho de rectificación, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:
  - La negativa del responsable del fichero a la rectificación de los datos solicitados.
  - Copia sellada por el responsable del fichero del modelo de petición de rectificación.
  - Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
  - Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud.

## EJERCICIO DEL DERECHO DE CANCELACIÓN<sup>(1)</sup>

### DATOS DEL RESPONSABLE DEL FICHERO

**Código de la unidad tramitadora:** U2800039

Departamento de Política Jurídica de Seguridad de la Información

**Nombre / razón social:** Universidad Nacional de Educación a Distancia (UNED)

**Dirección ante la que se ejercita el derecho de acceso:** Calle Bravo Murillo nº 38 28015-MADRID

CIF: Q2818016D

### DATOS DEL INTERESADO O REPRESENTANTE LEGAL<sup>(2)</sup>

**Nombre y Apellidos**

**Teléfono**

**Correo electrónico**

**Domicilio**

**C.P.**

**Localidad y Provincia**

**Con DNI nº**

del que acompaña copia, por medio del presente escrito ejerce el derecho de cancelación, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 31 y 32 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma y en consecuencia,

### **SOLICITA,**

Que se proceda a acordar la cancelación de los datos personales:

sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la cancelación practicada.

Que en caso de que se acuerde que no procede acceder al derecho, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la LOPD.

En

a de

de 20.....

Firmado,

1 Consiste en la petición de cancelación de datos que resulten innecesarios o no pertinentes para la finalidad con la que fueron recabados. Los datos serán bloqueados, es decir, serán identificados y reservados con el fin de impedir su tratamiento.

2 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero

## Instrucciones para el cumplimiento del formulario

1. Este modelo se utilizará por el afectado cuando desee cancelar o bloquear datos existentes en un fichero.

Sin perjuicio del ejercicio del derecho de cancelación a tenor del art. 16.5 de la Ley Orgánica 15/1999, los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

2. Debido al carácter personalísimo de los datos de carácter personal, es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad del afectado y sea considerado válido en derecho, de modo que el responsable del fichero pueda constatarla. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

3. La cancelación de los datos es **gratuita**.

4. Para que la [Agencia Española de Protección de Datos](#) pueda iniciar el procedimiento de tutela de derechos, resulta necesario que hayan transcurrido diez días hábiles desde la presentación de la solicitud por la que se ejercita el derecho de cancelación, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:

- La negativa del responsable del fichero a la cancelación de los datos solicitados.
- Copia sellada por el responsable del fichero del modelo de petición de cancelación.
- Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
- Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud.

## EJERCICIO DEL DERECHO DE OPOSICIÓN <sup>(1)</sup>

### DATOS DEL RESPONSABLE DEL FICHERO

**Código de la unidad tramitadora:** U2800039

Departamento de Política Jurídica de Seguridad de la Información

**Nombre / razón social:** Universidad Nacional de Educación a Distancia (UNED)

**Dirección ante la que se ejercita el derecho de acceso:** Calle Bravo Murillo nº 38 28015-MADRID

CIF: Q2818016D

### DATOS DEL INTERESADO O REPRESENTANTE LEGAL <sup>(2)</sup>

**Nombre y Apellidos**

**Teléfono**

**Correo electrónico**

**Domicilio**

**C.P.**

**Localidad y Provincia**

**Con DNI nº**

del que acompaño copia, por medio del presente escrito ejerzo el derecho de oposición, de conformidad con lo previsto en los artículos 6.4, 17 y 30.4 de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de carácter personal y en los artículos 34 y 35 del Real Decreto 1720/2007, de 21 de diciembre, que la desarrolla y en consecuencia,

### **EXPONGO,**

*(Describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo)*

Para acreditar la situación descrita, acompaño una copia de los siguientes documentos:

*(Enumerar los documentos que adjunta con esta solicitud para acreditar la situación que ha descrito)*

### **SOLICITO,**

Que sea atendido mi ejercicio del derecho de oposición, en el plazo de 10 días a contar desde la recepción de esta solicitud, en los términos anteriormente expuestos.

En

a de

de 20

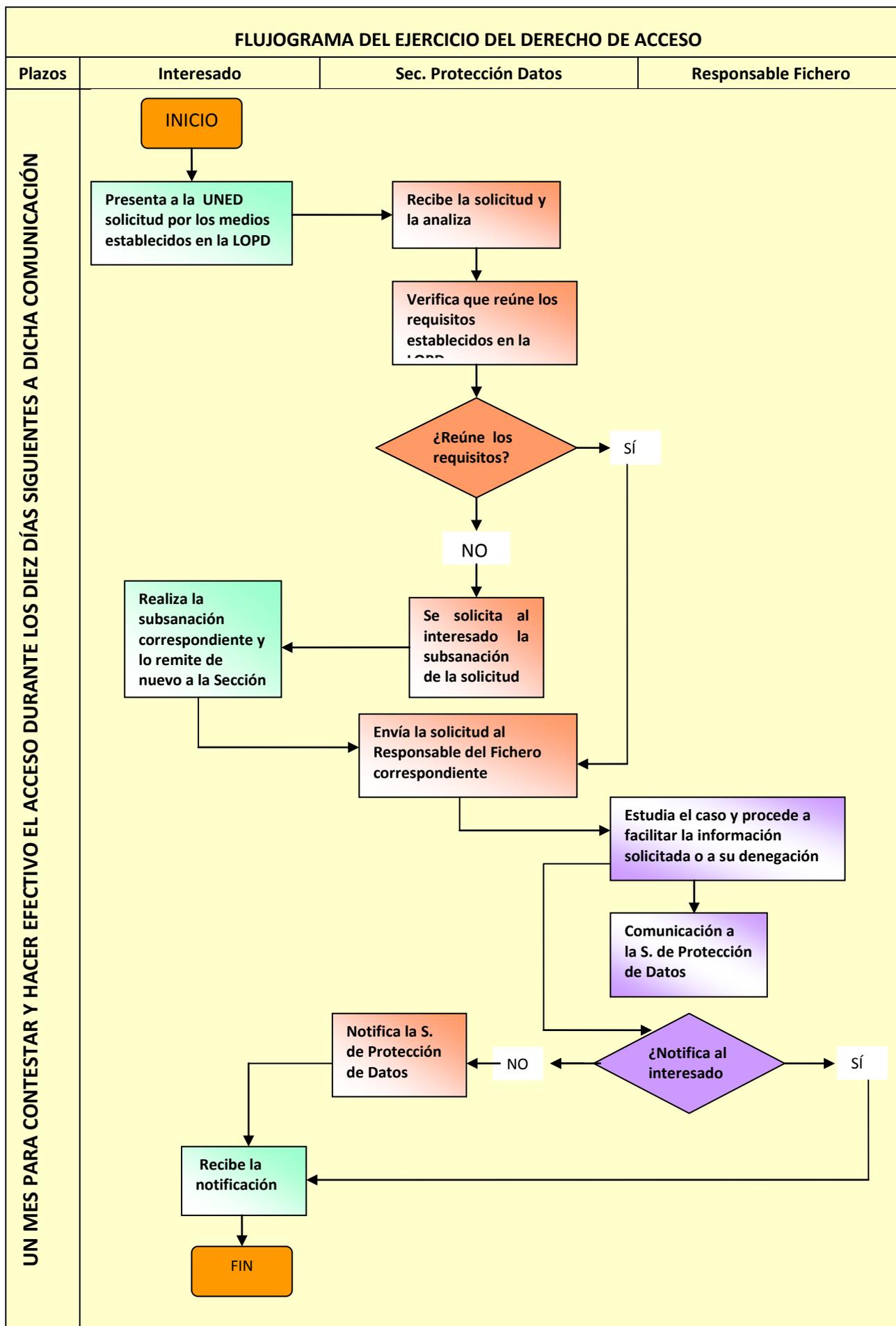
Firmado,

1 Se trata de la solicitud de oposición al tratamiento de los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Universidad Nacional de Educación a Distancia) que es quien dispone de los datos.

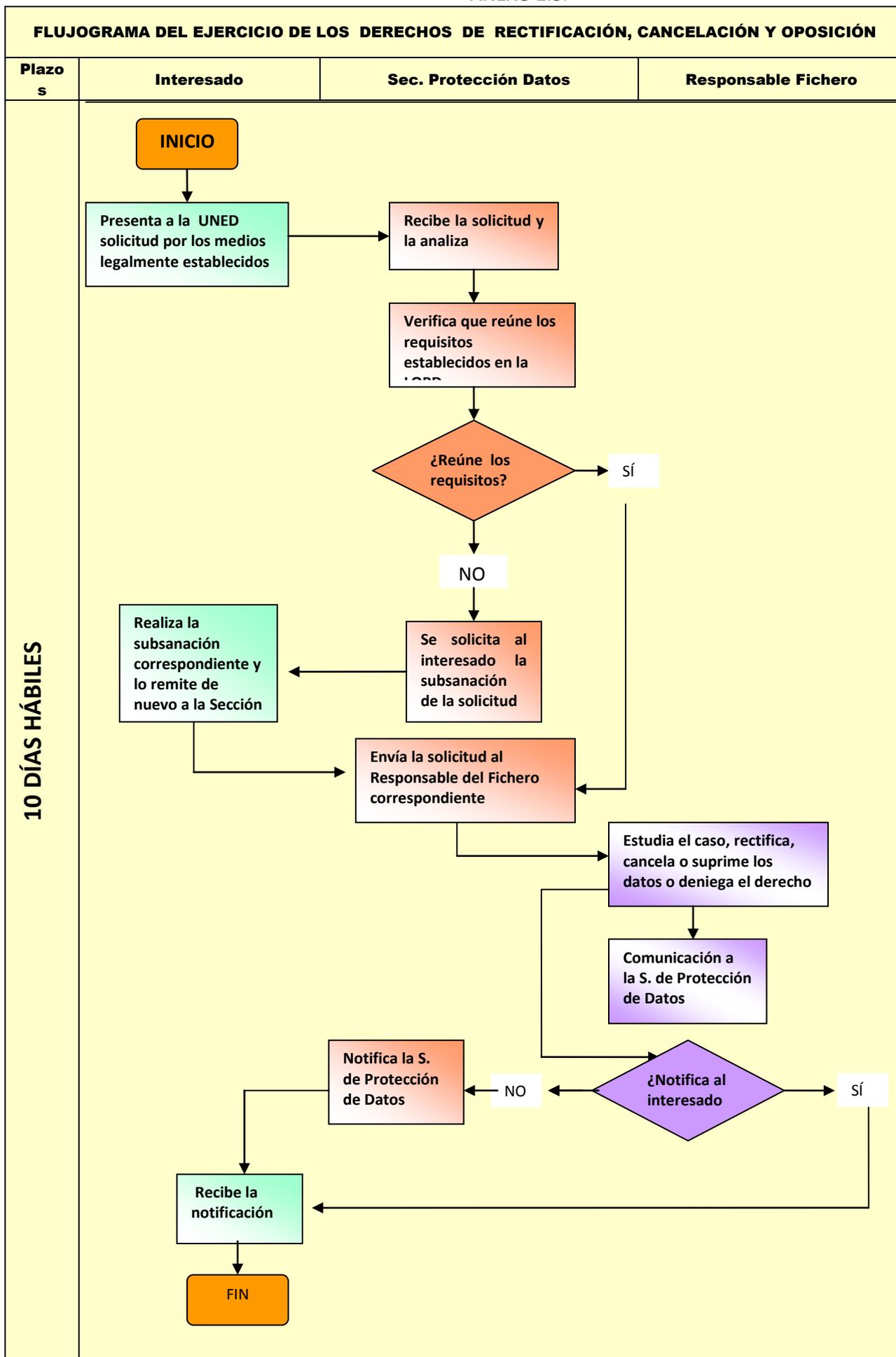
2 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero

## Instrucciones para el cumplimiento del formulario

1. Este modelo se utilizará por el afectado cuando desee oponerse a determinados tratamientos específicos de datos personales existentes en un fichero.
2. Para oponerse a un tratamiento de los datos que figuran en los ficheros resulta necesaria la existencia de unos motivos fundados y legítimos.
3. Debido al carácter personalísimo de los datos de carácter personal, es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad del afectado y sea considerado válido en derecho, de modo que el responsable del fichero pueda constatarla. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.
4. Para que la [Agencia Española de Protección de Datos](#) pueda iniciar el procedimiento de tutela de derechos, resulta necesario que hayan transcurrido diez días hábiles desde la presentación de la solicitud por la que se ejercita el derecho de oposición, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:
  - La negativa del responsable del fichero a la oposición de los datos solicitada.
  - Copia sellada por el responsable del fichero del modelo de petición de oposición.
  - Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
  - Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud.
5. La exclusión del tratamiento de los datos es **gratuita**.



ANEXO 1.3.



**ANEXO 1.4.****RELACIÓN DE RESPONSABLES DE FICHEROS PARA EL EJERCICIO DE LOS DERECHOS ARCO**

A continuación se relacionan los Responsables de Ficheros encargados de tramitar las solicitudes de ejercicio de derechos, cuando las mismas versen sobre información contenida en el fichero que le ha sido asignado

- 1. FICHERO ACCESO A LA INFORMACIÓN PÚBLICA**  
Responsable: Unidad de Análisis de procedimientos y modernización administrativa  
Calle Bravo Murillo, 38, 28015 -MADRID-
- 2. FICHERO DE ACCESO A LA UNIVERSIDAD**  
Responsable: Servicio de Acceso a la Universidad Calle Juan del Rosal, 14, 28040 -MADRID-
- 3. FICHERO ACTIVIDADES CULTURALES**  
Responsable: Vicegerencia de CC.AA. y atención al Estudiante Calle Bravo Murillo, 38, 28015 -MADRID-
- 4. FICHERO ADMISIONES**  
Responsable: Servicio de Ordenación Académica  
Calle Bravo Murillo, 38, 28015 -MADRID-
- 5. FICHERO ALUMNOS UNED-ABIERTA**  
Responsable: Dirección UNED-ABIERTA  
Calle Juan del Rosal, 14, 28040 -MADRID-
- 6. FICHERO ARCHIVO**  
Responsable: Archivo  
Calle Juan del Rosal, 14, 28040 -MADRID-
- 7. FICHERO BECAS AL ESTUDIANTE**  
Responsable: Servicio de Estudiantes  
Calle Bravo Murillo, 38 28015 -MADRID-
- 8. FICHERO BECAS AL FONDO SOCIAL**  
Responsable: Servicio de Estudiantes  
Calle Bravo Murillo, 38, 28015 -MADRID-
- 9. FICHERO BIBLIOTECA**  
Responsable: Biblioteca  
Calle Senda del Rey, 5, 28040 -MADRID-

**10. FICHERO BOLSAEMPLEO**

Responsable: Servicio de Estudiantes  
c/ Bravo Murillo, 38, 28015-MADRID-

**11. FICHERO CEMAV**

Responsable: CEMAV (Centro de Medios Audiovisuales)  
Calle Juan del Rosal, 12, 28040 -MADRID-

**12. FICHERO CONSULTAS DEL COIE**

Responsable: Servicio de Estudiantes  
Calle Bravo Murillo, 38 28015 -MADRID-

**13. FICHERO CONTROL ACCESOS**

Responsable: Departamento de Servicios Generales y Contratación  
Calle Bravo Murillo, 38, 28015 -MADRID-

**14. FICHERO CONTROL HORARIO**

Responsable: Vicegerencia de Recursos Humanos y organización  
Calle Bravo Murillo 38, 28015 -MADRID-

**15. FICHERO CUID**

Responsable: Departamento de Aprendizaje Permanente  
Calle Juan del Rosal, 14, 28040 -MADRID-

**16. FICHERO DEPORTES**

Responsable: Vicegerencia de CC.AA. y atención al Estudiante  
Calle Bravo Murillo, 38 28015 -MADRID-

**17. FICHERO EDITORIAL UNED**

Responsable: Editorial UNED  
Calle Juan del Rosal, 14, 28040 -MADRID-

**18. FICHERO ESTUDIANTES CENTROS PENITENCIARIOS**

Responsable: Servicio de Estudiantes  
Calle Bravo Murillo, 38, 28015 -MADRID-

**19. FICHERO ESTUDIANTES CURSO IBEROAMERICANO**

Responsable: Sección de Gestión de Recursos para la Docencia  
Calle Juan del Rosal 10, Facultad Psicología 28040 -MADRID-

**20. FICHERO EVALUACIÓN ACTIVIDAD ACADÉMICA UNIVERSITARIA**

Responsable: Oficina de Tratamiento de la Información  
Calle Bravo Murillo, 38, 28015 -MADRID-

**21. FICHERO EXPEDIENTE ACADÉMICO DE DOCTORADO**

Responsable: Administración de la Escuela de Doctorado  
Calle Bravo Murillo, 38, 28015 -MADRID-

**22. FICHERO GESTIÓN ACADÉMICA DE DOCTORADO**

Responsable: Administración de la Escuela de Doctorado  
Calle Bravo Murillo, 38, 28015 -MADRID-

**23. FICHERO GESTIÓN ACADÉMICA. DIPLOMATURAS, LICENCIATURAS Y GRADOS**

Responsable: Servicio de Ordenación Académica  
Calle Bravo Murillo, 38, 28015 -MADRID-

**24. FICHERO GESTIÓN ACADÉMICA. MÁSTERES UNIVERSITARIOS**

Responsable: Servicio de Posgrados Oficiales  
Calle Bravo Murillo, 38, 28015 -MADRID-

**25. FICHERO GESTIÓN DEL DOMINIO uned.es EN LA NUBE**

Responsable: Dirección del Centro de Tecnología de la UNED  
Carretera de las Rozas al Escorial, km.5 28230-Las Rozas\_ (Madrid)

**26. FICHERO GESTIÓN DE PERSONAL, ECONÓMICA Y ADMINISTRATIVA UNIVERSITASXXI-RECURSOS HUMANOS**

Responsable: Vicegerencia de Recursos Humanos y organización  
Calle Bravo Murillo, 38, 28015 -MADRID-

**27. FICHERO GESTIÓN DE TÍTULOS OFICIALES**

Responsable: Servicio de Ordenación Académica  
Calle Bravo Murillo, 38, 28015 -MADRID-

**28. FICHERO GESTIÓN DEL CORREO ELECTRÓNICO DEL PAS, PDI Y TUTORES**

Responsable: Dirección del Centro de Tecnología de la UNED  
Carretera de las Rozas al Escorial, km. 5 28230 -Las Rozas- (Madrid)

**29. FICHERO GESTIÓN DEL SERVICIO DE PSICOLOGÍA APLICADA (SPA)**

Responsable: Decanato de la Facultad Psicología  
Calle Juan del Rosal, 10, 28040 -MADRID-

**30. FICHERO GESTIÓN ECONÓMICA E INVENTARIO DE LA UNIVERSIDAD**

Responsable: Vicegerencia Económica y de Servicios Generales  
Calle Bravo Murillo, 38 28015 -MADRID-

**31. FICHERO GESTIÓN INVESTIGACIÓN**

Responsable: Departamento de Investigación y Apoyo a la Docencia  
Calle Bravo Murillo, 38, 28015 -MADRID-

**32. FICHERO GESTUVA**

Responsable: CINDETEC  
Carretera de las Rozas al Escorial, km. 5 28230 -Las Rozas- (Madrid)

**33. FICHERO OFICINA DEFENSOR UNIVERSITARIO**

Responsable: Defensor Universitario  
Calle Juan del Rosal, 16, E.T.S. de Ingeniería Informática 28040 -MADRID-

**34. FICHERO PREVENCIÓN DE RIESGOS LABORALES**

Responsable: Vicegerencia de Recursos Humanos y organización  
Calle Bravo Murillo, 38, 28015 -MADRID-

**35. FICHERO PROFESORES-TUTORES Y EXTENSIÓN UNIVERSITARIA**

Responsable: Vicegerencia de Centros Asociados y atención al Estudiante  
Calle Bravo Murillo, 38, 28015 -MADRID-

**36. FICHERO PRUEBAS PRESENCIALES**

Responsable: Servicio de Secretaría General  
Calle Bravo Murillo, 38, 28015 -MADRID-

**37. FICHERO QUEJAS Y SUGERENCIAS**

Responsable: Servicio de Atención Personalizada  
Calle Bravo Murillo, 38, 28015 -MADRID-

**38. FICHERO RECURSOS HUMANOS. IGUALDAD Y ACCIÓN SOCIAL**

Responsable: Vicegerencia de Recursos Humanos y organización  
Calle Bravo Murillo, 38 28015 -MADRID-

**39. FICHERO REGISTRO GENERAL**

Responsable: Servicio de Secretaría General  
Calle Bravo Murillo, 38, 28015 -MADRID-

**40. FICHERO RELACIONES INTERNACIONALES**

Responsable: Servicio de Internacionalización y Cooperación  
Calle Bravo Murillo, 38, 28015 -MADRID-

**41. FICHERO SERVICIO DE INSPECCIÓN**

Responsable: Dirección del Servicio de Inspección  
Calle Bravo Murillo, 38, 28015 -MADRID-

**42. FICHERO TARJETAS IDENTIFICATIVAS PERSONAL UNED**

Responsable: Vicegerencia de Recursos Humanos y organización  
Calle Bravo Murillo, 38, 28015 -MADRID-

**43. FICHERO TÍTULOS PROPIOS**

Responsable: Departamento de Aprendizaje Permanente  
Calle Juan del Rosal, 14, 28040 -MADRID-

**44. FICHERO UNIDIS. ESTUDIANTES CON DISCAPACIDAD**

Responsable: Servicio de Estudiantes  
Calle Bravo Murillo, 38 28015 -MADRID-

**45. FICHERO USUARIOS WEB**

Responsable: Centro de Tecnología de la UNED

Carretera de las Rozas al Escorial, Km.5 28230 -Las Rozas- (Madrid)

**46. FICHERO VIDEOVIGILANCIA**

Responsable: Departamento de Servicios Generales y Contratación

Calle Bravo Murillo, 38, 28015 -MADRID-

**EJERCICIO DEL DERECHO DE ACCESO**<sup>(1)</sup>

**DATOS DEL RESPONSABLE DEL FICHERO**

**Código de la unidad tramitadora:** U2800039

Departamento de Política Jurídica de Seguridad de la Información

**Nombre / razón social:** Universidad Nacional de Educación a Distancia (UNED)

**Dirección ante la que se ejercita el derecho de acceso:** Calle Bravo Murillo, nº 38 28015-MADRID

CIF: Q2818016D

**DATOS DEL INTERESADO O REPRESENTANTE LEGAL**<sup>(2)</sup>

**Nombre y Apellidos**

**Teléfono**

**Correo electrónico**

**Domicilio**

**C.P.**

**Localidad y Provincia**

**Con DNI nº**

del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 27 y 28 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma y en consecuencia,

**SOLICITA,**

Que se le facilite gratuitamente el derecho de acceso a sus datos contenidos en los ficheros titularidad de la UNED en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se me remita por correo la información en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso. Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los usos y finalidades para los que se almacenaron.

En

a

de

de 20

Firmado,

<sup>1</sup> Se trata de la petición de información sobre los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Universidad Nacional de Educación a Distancia) que es quien dispone de los datos.

<sup>2</sup> También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero

## Instrucciones para el cumplimiento del formulario

1. Es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad y sea considerado válido en derecho, para que el responsable del fichero pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.
2. El derecho de acceso **no podrá llevarse a cabo en intervalos inferiores a 12 meses**, salvo interés legítimo debidamente justificado.
3. Para que la [Agencia Española de Protección de Datos](#) pueda iniciar el procedimiento de tutela de derechos, resulta necesario que haya transcurrido un mes desde la presentación de la solicitud por la que se ejercita el derecho de acceso, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:
  - La negativa del responsable del fichero a facilitar la información solicitada.
  - Copia sellada por el responsable del fichero del modelo de petición de acceso.
  - Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
  - Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud.

### EJERCICIO DEL DERECHO DE RECTIFICACIÓN <sup>(1)</sup>

#### DATOS DEL RESPONSABLE DEL FICHERO

**Código de la unidad tramitadora:** U2800039

Departamento de Política Jurídica de Seguridad de la Información

**Nombre / razón social:** Universidad Nacional de Educación a Distancia (UNED)

**Dirección ante la que se ejercita el derecho de acceso:** C/ Bravo Murillo nº 38. 28015-MADRID

CIF: Q2818016D

#### DATOS DEL INTERESADO O REPRESENTANTE LEGAL <sup>(2)</sup>

**Nombre y Apellidos**

**Teléfono**

**Correo electrónico**

**Domicilio**

**C.P.**

**Localidad y Provincia**

**Con DNI nº**

que acompaña copia, por medio del presente escrito ejerce el derecho de rectificación sobre los datos anexos, aportando los correspondientes justificantes, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 31 y 32 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma y en consecuencia,

#### **SOLICITA,**

Que se proceda a acordar la rectificación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Que en caso de que se acuerde que no procede acceder al derecho, se me comuniqué motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la LOPD.

En

a

de

de 20

Firmado,

<sup>1</sup> Consiste en la petición dirigida al responsable del fichero (Universidad Nacional de Educación a Distancia) con el fin de que los datos personales respondan con veracidad a la situación actual del afectado.

<sup>2</sup> También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero

## Instrucciones para el cumplimiento del formulario

1. Este modelo se utilizará para el caso de que se deban rectificar datos inexactos o incompletos en un fichero.
2. Para probar el carácter inexacto o incompleto de los datos que figuran en los ficheros resulta necesaria la aportación de la documentación que lo acredite al responsable del fichero.
3. Debido al carácter personalísimo de los datos de carácter personal, es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad del afectado y sea considerado válido en derecho, de modo que el responsable del fichero pueda constatarla. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.
4. La rectificación de los datos es **gratuita**.
5. Para que la [Agencia Española de Protección de Datos](#) pueda iniciar el procedimiento de tutela de derechos, resulta necesario que hayan transcurrido diez días hábiles desde la presentación de la solicitud por la que se ejercita el derecho de rectificación, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:
  - La negativa del responsable del fichero a la rectificación de los datos solicitados.
  - Copia sellada por el responsable del fichero del modelo de petición de rectificación.
  - Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
  - Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud.

**EJERCICIO DEL DERECHO DE CANCELACIÓN<sup>(1)</sup>**

**DATOS DEL RESPONSABLE DEL FICHERO**

**Código de la unidad tramitadora:** U2800039

Departamento de Política Jurídica de Seguridad de la Información

**Nombre / razón social:** Universidad Nacional de Educación a Distancia (UNED)

**Dirección ante la que se ejercita el derecho de acceso:** Calle Bravo Murillo nº 38 28015-MADRID

CIF: Q2818016D

**DATOS DEL INTERESADO O REPRESENTANTE LEGAL<sup>(2)</sup>**

**Nombre y Apellidos**

**Teléfono**

**Correo electrónico**

**Domicilio**

**C.P.**




**SOLICITA,**

Que se proceda a acordar la cancelación de los datos personales:

sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la cancelación practicada.

Que en caso de que se acuerde que no procede acceder al derecho, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la LOPD.

En

 a  de  de 20 

Firmado,

1 Consiste en la petición de cancelación de datos que resulten innecesarios o no pertinentes para la finalidad con la que fueron recabados. Los datos serán bloqueados, es decir, serán identificados y reservados con el fin de impedir su tratamiento.

2 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero

## Instrucciones para el cumplimiento del formulario

1. Este modelo se utilizará por el afectado cuando desee cancelar o bloquear datos existentes en un fichero.

Sin perjuicio del ejercicio del derecho de cancelación a tenor del art. 16.5 de la Ley Orgánica 15/1999, los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

2. Debido al carácter personalísimo de los datos de carácter personal, es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad del afectado y sea considerado válido en derecho, de modo que el responsable del fichero pueda constatarla. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

3. La cancelación de los datos es **gratuita**.

4. Para que la [Agencia Española de Protección de Datos](#) pueda iniciar el procedimiento de tutela de derechos, resulta necesario que hayan transcurrido diez días hábiles desde la presentación de la solicitud por la que se ejercita el derecho de cancelación, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:

- La negativa del responsable del fichero a la cancelación de los datos solicitados.
- Copia sellada por el responsable del fichero del modelo de petición de cancelación.
- Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
- Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud.

**EJERCICIO DEL DERECHO DE OPOSICIÓN**<sup>(1)</sup>

**DATOS DEL RESPONSABLE DEL FICHERO**

**Código de la unidad tramitadora:** U2800039

Departamento de Política Jurídica de Seguridad de la Información

**Nombre / razón social:** Universidad Nacional de Educación a Distancia (UNED)

**Dirección ante la que se ejercita el derecho de acceso:** Calle Bravo Murillo nº 38 28015-MADRID

CIF: Q2818016D

**DATOS DEL INTERESADO O REPRESENTANTE LEGAL**<sup>(2)</sup>

Nombre y Apellidos

Correo electrónico



Domicilio

C.P.




**EXPONGO,**

*(Describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo)*

Para acreditar la situación descrita, acompaño una copia de los siguientes documentos:

*(Enumerar los documentos que adjunta con esta solicitud para acreditar la situación que ha descrito)*

**SOLICITO,**

Que sea atendido mi ejercicio del derecho de oposición, en el plazo de 10 días a contar desde la recepción de esta solicitud, en los términos anteriormente expuestos.

En  a  de  de 20

Firmado,

1 Se trata de la solicitud de oposición al tratamiento de los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Universidad Nacional de Educación a Distancia) que es quien dispone de los datos.

2 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero

## Instrucciones para el cumplimiento del formulario

1. Este modelo se utilizará por el afectado cuando desee oponerse a determinados tratamientos específicos de datos personales existentes en un fichero.
2. Para oponerse a un tratamiento de los datos que figuran en los ficheros resulta necesaria la existencia de unos motivos fundados y legítimos.
3. Debido al carácter personalísimo de los datos de carácter personal, es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad del afectado y sea considerado válido en derecho, de modo que el responsable del fichero pueda constatarla. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.
4. Para que la [Agencia Española de Protección de Datos](#) pueda iniciar el procedimiento de tutela de derechos, resulta necesario que hayan transcurrido diez días hábiles desde la presentación de la solicitud por la que se ejercita el derecho de oposición, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:
  - La negativa del responsable del fichero a la oposición de los datos solicitada.
  - Copia sellada por el responsable del fichero del modelo de petición de oposición.
  - Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
  - Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud.
5. La exclusión del tratamiento de los datos es **gratuita**.



## ANEXO 2.1.

### CLÁUSULA INFORMATIVA

De conformidad con La Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal le informamos que los datos personales por usted facilitados a través del presente formulario se incorporarán a un fichero titularidad de la Universidad Nacional de Educación a Distancia (UNED), cuya finalidad es la de

.....  
.....

Asimismo, los datos serán utilizados para enviar información, por cualquier medio, acerca de las finalidades antes descritas.

Sus datos no serán cedidos o comunicados a terceros, salvo en los supuestos necesarios para la debida atención, desarrollo, control y cumplimiento de las finalidades expresadas, así como en los supuestos previstos, según Ley.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.2.

## CLÁUSULA MATRÍCULA

## INFORMACIÓN RELATIVA A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De acuerdo con La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que al aceptar este documento da su conformidad para que los datos suministrados en el proceso de matrícula sean incluidos en un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED), cuya finalidad es la organización de la docencia y el estudio, así como el ejercicio de las demás funciones propias del Servicio Público de la Educación Superior, reguladas en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y en los Estatutos de la UNED.

Estos datos se comunicarán, cuando legalmente proceda, a los Centros Asociados a la UNED y a las Administraciones Públicas competentes en materia educativa. Asimismo, cuando se domicilie el pago de los precios públicos se comunicarán a las entidades bancarias los datos estrictamente necesarios para la realización de aquél.

**He sido informado y acepto...**



Asimismo, le informamos que sus datos podrán ser utilizados a fin de mantenerle informado, por cualquier medio de contacto, de los servicios, cursos y actividades organizadas por la UNED y/o las entidades directamente relacionadas con ésta. Para ello, deberá prestar su consentimiento marcando la siguiente casilla:

**Deseo recibir dicha información acerca de la UNED y las entidades directamente relacionadas con ésta.**



Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## **ANEXO 2.3.**

### **CLÁUSULA CARTA DE PAGO DE LA MATRÍCULA**

#### **(Información relativa a la Protección de Datos de Carácter Personal)**

De acuerdo con La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), le informamos que al aceptar este documento da su conformidad para que los datos suministrados en el proceso de matrícula sean incluidos en un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED), cuya finalidad es la organización de la docencia y el estudio, así como el ejercicio de las demás funciones propias del Servicio Público de la Educación Superior, reguladas en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y en los Estatutos de la UNED.

Estos datos se comunicarán, cuando legalmente proceda, a los Centros Asociados a la UNED y a las Administraciones Públicas competentes en materia educativa. Asimismo, he sido informado de que cuando se domicilie el pago de los precios públicos se comunicará, a las entidades bancarias, los estrictamente necesarios para la gestión del pago.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

#### ANEXO 2.4.

### CLÁUSULA DE ACEPTACIÓN PARA USO EDUCATIVO Y CULTURAL DE LA VOZ Y/O IMAGEN DE PARTICIPANTES EN LA DIFUSIÓN DE CONTENIDOS AUDIOVISUALES DE LA UNED

Madrid \_\_\_\_de\_\_\_\_de 20\_\_\_\_

D/D<sup>a</sup> \_\_\_\_\_

Autorizo al Centro de Medios Audio-Visuales (CEMAV), a la difusión de mi VOZ y/o IMAGEN registrada/s en la/s grabación/es, que se realicen sin fines lucrativos para la difusión y la transferencia del conocimiento al servicio de la cultura y el desarrollo económico, a través de los medios audiovisuales de comunicación que utiliza habitualmente la UNED (RTVE, Internet, Intranet, DVD, CD audio, jornadas, eventos u otros medios empleados por la Universidad).

Fdo:

## ANEXO 2.5.

### MODELO CLÁUSULA CEMAV –AUTORIZACION DE LAS GRABACIONES

De conformidad con La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que sus datos personales serán incorporados en un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED), cuya finalidad es la de gestionar las autorizaciones de los invitados que participen en programas de Radio, Televisión u otros medios. Para ello se consiente el tratamiento de su imagen y/o voz para su almacenamiento y en su caso, posterior utilización.

Asimismo, le informamos de que sus datos personales podrán ser comunicados a los titulares de los medios en los que participe, para el desarrollo, control y cumplimiento de las finalidades expresadas, así como en los supuestos previstos en la Ley.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.6.

### MODELO CLÁUSULA CEMAV – PROGRAMAS RADIO Y TV

De conformidad con La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que los datos personales facilitados a través del presente impreso se incluirán en un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED), cuya finalidad es la de gestionar la participación en programas de Radio, Televisión u otros medios, así como las autorizaciones y liquidaciones de las compensaciones económicas que pudieran acordarse por su intervención en calidad de conferenciante de la UNED.

Sus datos serán cedidos o comunicados a los titulares de los medios en los que participe, para el desarrollo, control y cumplimiento de las finalidades expresadas, así como en los supuestos previstos, según Ley.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.7.

### SEGURIDAD Y CONTROL DE ACCESOS AL EDIFICIO

#### (Protección de Datos)

Dado que la recogida de datos personales, a los efectos de la seguridad y control de acceso al edificio, se realiza por la transmisión oral al Vigilante Jurado y, la transcripción por éste de la información a soporte papel, un mecanismo apropiado para cumplir con la obligación es la exhibición de un rótulo con el texto legal en el propio mostrador de la entrada. Así, se aporta la siguiente propuesta de rótulo:

#### CLÁUSULA CONTROL DE ACCESOS

Le informamos que los datos de carácter personal recabados son incorporados a un fichero titularidad de la Universidad Nacional de Educación a Distancia (UNED), cuya finalidad es la seguridad y control de acceso al edificio de la Institución.

La no comunicación de los datos solicitados puede provocar la denegación del acceso al edificio. Asimismo, le informamos que sus datos no serán comunicados a terceros, salvo en aquellos supuestos en que sea estrictamente necesario para el cumplimiento de los fines que motivan su recogida o aquellos legalmente previstos.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.8.

### CLÁUSULA INFORMATIVA SOBRE PROTECCIÓN DE DATOS PERSONALES PARA LOS EMPLEADOS

De conformidad con La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), le informamos de que los datos personales aportados por usted para la formalización de la relación funcional o contractual son integrados en un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED).

La recogida y tratamiento de la información de carácter personal, responde, de forma general, a las siguientes finalidades y usos:

- **RECURSOS HUMANOS Y GESTIÓN DE NÓMINAS.-** Gestión, Selección, Promoción y/o Formación; Prestaciones Sociales; Seguros; Gestión de nóminas y otros tipos de retribuciones. Gestión de Personal (Altas, Bajas, Planes de Pensiones, Comisiones de servicio, Haberes, Trienios, Permisos y licencias, Vacaciones, Control de asistencia, Formación, Anticipos, Ayudas Sociales, así como otros aspectos del ámbito laboral y funcional).
- **PREVENCIÓN DE RIESGOS LABORALES.-** Gestión de la Prevención de Riesgos Laborales, con tratamiento de información relativa al puesto de trabajo y situaciones de riesgo, así como formación en la materia.
- **SERVICIO MÉDICO O VIGILANCIA DE LA SALUD.-** La gestión y control de servicios de vigilancia de la salud. En este caso, los datos personales serán tratados, única y exclusivamente, por personal sanitario y/o sometidos al deber de secreto o sigilo profesional propio de la/s entidad/es contratada/s a estos efectos; no teniendo la UNED acceso a esta información de carácter personal, conforme establece la legislación en materia de Prevención de Riesgos Laborales.

De este modo, los resultados de las pruebas médicas a las que sea sometido el trabajador, sólo serán comunicados al interesado, de forma confidencial. La UNED, única y exclusivamente, será informada acerca de la aptitud para el desempeño del puesto de trabajo.

- **FORMACIÓN.-** Gestión de las solicitudes, inscripciones o matriculación en cursos, seminarios, jornadas o conferencias de carácter formativo, con carácter voluntario u obligatorio, presencial o a distancia, control de asistencia y entrega o expedición de títulos, diplomas o certificados.

- **VIDEOVIGILANCIA.**- En las dependencias de la UNED se ha procedido a la instalación de cámaras de Videovigilancia cuya única finalidad responde a poder garantizar la seguridad de las instalaciones, del material ubicado en las mismas, así como del personal que se encuentre en las mismas.

Los datos objeto de tratamiento no serán cedidos o comunicados a terceros, salvo en los supuestos necesarios para el estricto y exclusivo cumplimiento o satisfacción de las finalidades antes mencionadas, así como en los legalmente previstos. De esta manera, los datos personales serán cedidos, sin consentimiento de su titular, de acuerdo con el artículo 11.1 LOPD en los casos siguientes:

- La información de carácter fiscal y laboral será comunicada a los Organismos de la Seguridad Social, Administración Tributaria, Servicios Públicos de empleo estatal, Autoridad Laboral, Órganos de representación de los Empleados Públicos, así como en los supuestos previstos y fijados por la normativa aplicable.

- En su caso, serán cedidos los datos personales a las Compañías Aseguradoras con las cuales, en su caso, se haya contratado, entre otros, un seguro de vida, accidentes y/o servicios para la salud, en los que usted sea beneficiario.

- Si durante la vigencia de la relación con esta Administración educativa, usted es seleccionado para asistir a cursos de formación, sus datos personales serán cedidos al docente y/o centro donde se impartirán, a efectos de mantener un control de los asistentes y, en su caso, emitir la certificación de asistencia o expedición del título o diploma respectivo.

De acuerdo con la citada normativa, está obligado a informar de las variaciones que puedan experimentar los datos personales facilitados.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

Fecha:

Firmado:

NOMBRE Y APELLIDOS DEL EMPLEADO

## ANEXO 2.9.

### CLÁUSULA CONVENIOS

#### DE LOS DATOS FACILITADOS POR EL PRESTADOR DE SERVICIOS

De conformidad con La Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal le informamos que los datos personales facilitados, para los casos en que éste sea una persona física, o en el caso de representantes de una persona jurídica, ya sea pública o privada, serán incorporados a un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED).

La finalidad de la recogida y tratamiento de la información es la gestión del acuerdo suscrito en el cuerpo del presente escrito, así como el mantenimiento del contacto de ambas partes.

En cumplimiento de la normativa vigente, la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED) garantiza que ha adoptado las medidas técnicas y organizativas necesarias para mantener el nivel de seguridad requerido, en atención a la naturaleza de los datos personales tratados.

Asimismo, la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED) informa que no cederá o comunicará los datos personales almacenados en sus ficheros a terceros, salvo en los supuestos legalmente previstos o cuando fuere necesario para la prestación del servicio.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.10.

Este modelo se incorporará al formulario normalizado de curriculum elaborado por la UNED. En el caso de no poder facilitar en el momento, copia del formulario a la persona que facilita los datos, se le hará llegar de forma inmediata en un momento posterior a la recogida de datos.

### CLÁUSULA PARA QUIENES PRESENTAN CURRICULUM

En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa de que los datos personales aportados de forma voluntaria son incorporados en un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED), cuya finalidad es la gestión de solicitudes de empleo y, en su caso, el proceso selectivo en el que pudiera ser incluido, para la provisión de puestos de trabajo a través de la gestión de las bolsas de empleo o instrumentos similares, que la UNED ponga en marcha.

Los datos personales no serán cedidos o comunicados a terceros, salvo en los supuestos previstos, según Ley. La UNED conservará el currículum, por si en alguna ocasión fuese preciso cubrir algún puesto de trabajo en el área de su formación académica y/o profesional, hasta la revocación por parte del titular de los datos.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.11.

### CLÁUSULA DE AUTORIZACION DE LAS GRABACIONES EN AULAS AVIP

De conformidad con La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos de que sus datos personales serán incorporados a un fichero titularidad del Centro Asociado de la Universidad Nacional de Educación a Distancia (UNED) cuya finalidad es la de gestionar las autorizaciones de los participantes en grabaciones de clases, tutorías, conferencias y seminarios. Para ello se consiente el tratamiento de su imagen y/o voz para su almacenamiento y en su caso, posterior utilización.

Asimismo, le informamos que sus datos personales podrán ser comunicados para el desarrollo, control y cumplimiento de las finalidades expresadas, así como, en los supuestos previstos en la Ley.

En cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación y, en su caso oposición de sus datos, enviando una solicitud por escrito, adjuntando fotocopia de su DNI, dirigida al CC.AA. de la UNED .....

## ANEXO 2.12.

### CLÁUSULA PARA EL CORREO ELECTRÓNICO

**Nota.-** *El siguiente texto legal debiera ser contemplado en los mensajes de correo electrónico corporativo de la Institución \*\*\*@uned.es*

Este mensaje y los ficheros adjuntos pueden contener información confidencial. Los mismos contienen información reservada que no puede ser difundida. Si usted ha recibido este correo por error, tenga la amabilidad de eliminarlo de su sistema y avisar al remitente mediante reenvío a su dirección electrónica; no deberá copiar el mensaje ni divulgar su contenido a ninguna persona.

Su dirección de correo electrónico junto a sus datos personales, constan en un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED).

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.13.

### CLÁUSULA PRÁCTICAS FORMATIVAS-BECARIOS

En cumplimiento de La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se le informa de que los datos personales que nos ha facilitado serán incorporados a un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED), cuya finalidad es la gestión y tramitación de las solicitudes de personas interesadas en la realización de prácticas en calidad de becario en formación.

Los datos personales no serán cedidos o comunicados a terceros, salvo en los supuestos previstos, según Ley y los necesarios para el control, desarrollo y cumplimiento de su vinculación. En su caso, los datos económicos serán cedidos a la entidad bancaria o financiera con la que la UNED trabaje, para el correspondiente pago de las cuantías estipuladas.

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

Firmado:

NOMBRE Y APELLIDOS

## ANEXO 2.14.

### DEBER DE INFORMACIÓN EN RELACIÓN CON LA VIDEOVIGILANCIA

Partiendo de la premisa de que las imágenes son un dato de carácter personal, de acuerdo con lo establecido en el artículo 3 de la LOPD y el artículo 1.4 del Real Decreto 1322/1994, de 20 de junio, se aprobó la Instrucción 1/2006, de 8 de Noviembre, de la Agencia Española de Protección de Datos, sobre el Tratamiento de Datos Personales con fines de Vigilancia a través de sistemas de cámaras o videocámaras (BOE Núm. 296 de 12 diciembre 2006).

De conformidad con el artículo 3 de la Instrucción, los Responsables de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED), que cuenten con sistemas de Videovigilancia, deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

- a) Colocar, en las zonas video vigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados.
- b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999. El contenido y el diseño del distintivo informativo se ajustarán a lo previsto en el **Anexo** de esta Instrucción.

En cumplimiento de la mencionada norma se aporta, a continuación, el distintivo con el diseño y contenido regulado, así como el modelo de cláusula informativa, a tener a disposición de los interesados en el mostrador de entrada.

Cabe decir que la ubicación del distintivo estará en lugar visible para el interesado, el cual se exhibirá en lugar estratégico, donde se estime oportuno por la institución, sobre todo, en la puerta de acceso principal. De acuerdo con el Informe 0084/2007 de la AEPD, se resuelven varias cuestiones en cuanto a la interpretación y aplicación de la Instrucción 1/2006. Entre otras cuestiones, ésta es la respuesta textual de la AEPD:

- No existe ningún criterio de la Agencia, referido a las dimensiones, debiendo ser un cartel informativo acorde con el espacio en el que se vaya a ubicar, dado que no es equiparable colocar el cartel informativo en un autobús o en la entrada de un edificio.
- Respecto a su ubicación, no es necesario que se coloque debajo de la cámara, será suficiente conforme lo dispuesto en el artículo 3 a) de la citada Instrucción, colocar el distintivo informativo en lugar suficientemente visible, tanto en espacios abiertos como cerrados. Por tanto, resultaría aconsejable que, tratándose de un edificio sometido a videovigilancia, en la entrada del mismo, se ubicara el cartel informativo.

## ANEXO

**ZONA VIDEOVIGILADA**

**LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE  
DATOS DE CARÁCTER PERSONAL**

**PUEDE EJERCITAR LOS DERECHOS DE ACCESO Y CANCELACIÓN ANTE  
LA UNED. C/ Bravo Murillo, 38 28015-MADRID**

**MÁS INFORMACIÓN  
SOLICITAR EN MOSTRADOR *DE ENTRADA***

## CLÁUSULA INFORMATIVA DE VIDEOVIGILANCIA

De conformidad con lo dispuesto en el art. 5.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, se informa:

1. Que su imagen, como dato de carácter personal, se incorporará a un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED) y será tratado con la finalidad de preservar la seguridad, personal y material, en las diferentes sedes e instalaciones de la UNED, a través de un sistema de videovigilancia.
2. Que los destinatarios de estos datos personales (imágenes) pueden ser:
  - a. La empresa de seguridad contratada por la UNED.
  - b. Las Fuerzas y Cuerpos de Seguridad, así como la Administración de Justicia, en los supuestos legalmente previstos.
3. Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.15

**FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS**

En el trabajo diario es habitual la generación de **ficheros temporales** por parte de los usuarios para atender a distintas necesidades, es decir, ficheros obtenidos a partir de un fichero matriz o principal y que se crean, normalmente, en un procesador de texto (Microsoft Word) o en una hoja de cálculo (Microsoft Excel).

**Es importante recordar que** la utilización de estos ficheros requiere el cumplimiento de uno de los Principios de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), el de la **calidad de los datos**. En este sentido el art.4.3 señala que: *“los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado”*.

De no cumplir con este principio, estaríamos ante una infracción grave según el art.44.3 c) de la citada Ley.

Por ello, **todo fichero temporal o copia de trabajo será borrado o destruido una vez que haya dejado de ser necesario** para los fines que motivaron su creación. Al respecto, en la Normativa de seguridad y buen uso del Sistema de Información de la UNED se establece que **transcurrido un mes, si el usuario detecta la necesidad de continuar utilizando la información almacenada en el fichero, deberá comunicárselo al Responsable de seguridad**, para adoptar sobre el mismo las medidas oportunas.

## ANEXO 2.16

### CLÁUSULA DE CONSENTIMIENTO EN TRANSFERENCIAS INTERNACIONALES DE DATOS A TRAVÉS DE CONVENIOS

**Aviso**

El importe de la matrícula para los datos seleccionados es de 325 €.

Presione el botón **Aceptar** si desea continuar con la matrícula o **Cancelar** para modificar algún dato elegido.

Autorizo a la UNED la transferencia internacional de mis datos a la entidad que suscribe el convenio.

**Aceptar** **Cancelar**

---

**AVISO LEGAL**

---

**I. DATOS IDENTIFICATIVOS**

De acuerdo con el artículo 10 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, ponemos en su conocimiento la siguiente información:

1. El presente portal, **<http://www.uned.es>**, constituye el Sitio Oficial en Internet de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (en adelante, UNED).
2. La UNED es una institución pública educativa que fue creada por el Decreto 2310/1972, de 18 de agosto (BOE de 9 de septiembre de 1972).
3. La UNED está provista de CIF nº: Q-2818016-D
4. La sede del rectorado de la UNED se encuentra en la calle Bravo Murillo, 38 - 28015 de Madrid.
5. Los usuarios del presente portal podrán contactar con la UNED mediante comunicación escrita remitida a su domicilio social, indicado en el punto anterior.

**II. DERECHOS DE PROPIEDAD INTELECTUAL E INDUSTRIAL**

1. Tanto el diseño del Portal y sus códigos fuente, como los logos, marcas y demás signos distintivos que aparecen en el mismo, son titularidad de la UNED o entidades colaboradoras y están protegidos por los correspondientes derechos de propiedad intelectual e industrial.
2. Están prohibidas la reproducción, transformación, distribución, comunicación pública, puesta a disposición del público y, en general, cualquier otra forma de explotación, parcial o total de los elementos referidos en el apartado anterior. Estos actos de explotación sólo podrán ser realizados en virtud de autorización expresa y por escrito de la UNED y que, en todo caso, deberán hacer referencia explícita a la titularidad de los citados derechos de propiedad intelectual de la UNED. En ningún caso se podrán suprimir, alterar, eludir o manipular cualesquiera dispositivos de protección o sistemas de seguridad que puedan estar instalados. En particular, los materiales dispuestos por el personal docente a través del sitio Web serán para uso exclusivo de los estudiantes con fines educativos.
3. La UNED declara su respeto a los derechos de propiedad intelectual e industrial de terceros; por ello si considera que este sitio pudiera estar violando sus derechos, rogamos se ponga en contacto con la Universidad Nacional de Educación a Distancia.

## ANEXO 2.17

**III. PUBLICACIÓN DE IMÁGENES DE PERSONAS**

1. En relación con las imágenes de personas que aparecen en el sitio Web, la UNED efectúa la publicación respetando la Ley Orgánica 1/1982 de 5 de mayo, de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El Usuario no está autorizado a reproducir, distribuir y comunicar imágenes fotográficas y video gráficas. Estas imágenes son utilizadas, única y exclusivamente, en la composición de archivos gráficos o video gráficos, elaboradas para informar y dar a conocer diversas actividades de la Universidad.
3. El tratamiento de las imágenes de los estudiantes, del personal docente o del personal de administración y servicios, se efectúa respetando a la persona, eliminando cualesquiera captaciones o filmaciones que pudieren atentar los derechos fundamentales. Las imágenes no son utilizadas para otros fines distintos a los expresados, ni son cedidos a terceras personas, salvo las autorizadas al tratamiento.
4. En todo caso, la persona afectada por una publicación en el sitio Web de su imagen, podrá revocar el consentimiento que hubiese prestado, oponerse al tratamiento de la imagen, o ejercitar los derechos de acceso o cancelación, en cualquier momento, presentando o enviando un escrito, acompañado de la fotocopia de su DNI y una fotografía actualizada, a la UNED.

**IV. CONDICIONES Y TÉRMINOS DE USO DE LOS SITIOS WEB**

El Usuario se obliga al cumplimiento de las presentes condiciones y términos de uso:

1. No introducir, almacenar o difundir en los sitios Web, información o material que sea difamatorio, injurioso, obsceno, amenazador, xenófobo, incite a la violencia, a la discriminación por razón de raza, sexo, ideología, religión o que de cualquier forma atente contra la moral, el orden público, los derechos fundamentales, las libertas públicas, el honor, la intimidad o la imagen de terceros y en general la normativa vigente.
2. Custodiar adecuadamente el "Nombre de Usuario" (Login) y la "Contraseña" (Password) que le sea facilitada por la Universidad a los Usuarios, como elementos identificadores y habilitadores para el acceso a los distintos servicios ofrecidos en los sitios Web de la UNED, comprometiéndose a no ceder su uso ni a permitir el acceso a ellos de terceros, asumiendo la responsabilidad por los daños y perjuicios que pudieran derivarse de un uso indebido de los mismos.

## ANEXO 2.17

En virtud de lo anterior, es obligación del Usuario notificar, al Departamento de Sistemas de la UNED, cualquier hecho que permita el uso indebido de los identificadores y contraseñas, tales como el robo, extravío, o el acceso no autorizado a los mismos, con el fin de proceder a su inmediata cancelación. Mientras no se comuniquen tales hechos, la Universidad quedará eximida de cualquier responsabilidad que pudiera derivarse del uso indebido de los identificadores o contraseñas por terceros no autorizados.

3. No realizar actividades publicitarias, promocionales o de explotación comercial a través de los sitios Web.
4. No utilizar identidades falsas, ni suplantar la identidad de otros en la utilización del sitio Web o en la utilización de cualquiera de sus servicios, incluyendo la utilización en su caso de contraseñas o claves de acceso de terceros o de cualquier otra forma.
5. No destruir, alterar, utilizar para su uso, inutilizar o dañar los datos, informaciones, programas o documentos electrónicos de la UNED o terceros.

### **V. CONDICIONES Y TÉRMINOS DE USO PARTICULARES DE DETERMINADOS SERVICIOS**

Algunos servicios pertenecientes a la UNED disponen, por sus peculiaridades de condiciones y términos de uso particulares. A los mismos les serán de aplicación las condiciones generales aplicables enunciadas en el apartado anterior, mientras no se opongan a las condiciones particulares.

### **VI. EXONERACIÓN DE RESPONSABILIDAD DE LA UNED**

1. La UNED no se hace responsable, con carácter general, del uso inadecuado del sitio Web titularidad de la Universidad. Los Usuarios deberán realizar un uso adecuado del sitio Web, de acuerdo con las condiciones y términos anteriores, sin que la UNED pueda tener ninguna responsabilidad por la utilización indebida.
2. Respecto de posibles deficiencias técnicas.- La UNED no será responsable en ningún caso de las alteraciones en el servicio que se produzcan por fallos en la red eléctrica, en la red de conexión de datos, en el servidor o en cualesquiera prestaciones.
3. Respecto al acceso por terceros a su sistema, la UNED adoptará las cautelas técnicas necesarias a fin de proteger los datos e información a la que se accede, pero sin que sea responsable de actuaciones de terceros que, vulnerando las medidas de seguridad establecidas, accedan a los citados datos.
4. Respecto a la exactitud de la Información, las informaciones contenidas en el sitio Web han sido elaboradas exclusivamente con carácter divulgativo y no tienen valor oficial, salvo cuando así se indique.

## ANEXO 2.17

5. Las informaciones y contenidos existentes pueden ser cambiados o retirados sin previo aviso. Igualmente se podrán realizar mejoras o cambios en los productos, servicios, diseño o programas utilizados para su funcionamiento en cualquier momento y sin previo aviso
6. El sitio contiene enlaces (*links*) a otras páginas de terceros, cuyos contenidos no puede controlar en todo momento. La conexión de un Usuario desde el sitio con estos otros lugares de la red ajenos a nuestra Universidad se realizará, por tanto, bajo la exclusiva responsabilidad del navegante. No obstante, si observase en ellas cualquier información que pudiese resultar contraria a las leyes, a la dignidad de las personas, o de carácter racista, xenófobo o de apología del terrorismo o la violencia, rogamos que nos lo comunique con el fin de poder retirarla.

### VII. LEGISLACIÓN APLICABLE Y JURISDICCIÓN

Las presentes condiciones y términos, se regirán por las normas estatutarias, reglamentarias y por la legislación española, que será de aplicación en lo no dispuesto en este aviso legal en materia de interpretación, validez y ejecución.

Las partes renuncian expresamente al fuero que les pudiera corresponder y someten expresamente a los Juzgados y Tribunales de Madrid para resolver cualquier controversia que pueda surgir en la interpretación o ejecución de las presentes condiciones.

## ANEXO 2.18.

### POLÍTICA DE PRIVACIDAD

---

#### I. POLÍTICA DE PRIVACIDAD

La UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (en adelante UNED) está especialmente sensibilizada en la protección de los datos personales de los usuarios de los servicios, a los que se accede a través de su Web.

Mediante la presente Política de Privacidad, la UNED informa a los usuarios del sitio [www.uned.es](http://www.uned.es) del tratamiento y usos a los que se someten los datos de carácter personal que se recaban en la Web, con el fin de que decidan, libre y voluntariamente, si desean facilitar la información solicitada.

La UNED se reserva la facultad de modificar esta Política con el objeto de adaptarla a novedades legislativas, criterios jurisprudenciales, prácticas del sector, o intereses de la entidad. Cualquier modificación en la misma será anunciada con la debida antelación, a fin de que el usuario tenga perfecto conocimiento de su contenido.

Ciertos servicios prestados en el portal pueden contener condiciones particulares con previsiones específicas en materia de protección de datos personales, pudiendo informarse en los correspondientes apartados.

#### II. TITULARIDAD DEL TRATAMIENTO

Los datos de carácter personal que puedan ser suministrados a través del sitio Web serán incorporados a ficheros titularidad de la UNED, debidamente inscritos en el Registro General de Protección de Datos.

#### III. CONSENTIMIENTO DEL USUARIO

Mediante la presente Política, el usuario manifiesta que conoce, consiente y autoriza expresamente la incorporación de sus datos de carácter personal, al tratamiento de sus datos con los fines expresados.

#### IV. USOS Y FINALIDADES

La finalidad de la recogida y tratamiento de los datos personales es la gestión, prestación y personalización de los servicios y contenidos del mismo que el usuario utilice.

#### V. COMUNICACIÓN DE LOS DATOS

Los datos recabados a través de la Web sólo serán cedidos en aquellos casos en que expresamente se informe de ello al usuario.

## VI. SEGURIDAD DE LOS DATOS Y UTILIZACIÓN DE COOKIES

La UNED adopta las medidas de seguridad, según lo dispuesto en los artículos 89 a 114 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre. Asimismo, adopta las medidas técnicas y organizativas, que garanticen la seguridad de los datos de carácter personal y evitan su alteración, pérdida, tratamiento o acceso no autorizado.

La UNED emplea *cookies* cuando el usuario navega por su página Web, que son activadas desde el servidor [www.uned.es](http://www.uned.es)

Las *cookies* son pequeños ficheros de datos que se alojan en el terminal de la UNED y que contienen cierta información de la visita al sitio Web. La UNED utiliza *cookies* únicamente con el fin de facilitar la navegación de los Usuarios y sin que en ningún caso sea posible asociar tales *cookies* a los datos personales concretos de los usuarios ni identificar a éstos a través de aquéllas. Los usuarios tienen, no obstante, la posibilidad, existente en la mayoría de navegadores Web, de desactivar o eliminar estas *cookies*.

## VII. DERECHOS DE LOS USUARIOS

Le recordamos que en cualquier momento podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición de sus datos, ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la UNED.

## ANEXO 2.19

Cláusula a insertar en el perfil del contratante de la página Web titularidad de la UNED

### PERFIL DEL CONTRATANTE

**Nota.-** Se aporta a continuación, un modelo de cláusula informativa para que incluya en la página Web titularidad de la UNED, espacio "empresas", en el apartado relativo al "perfil del contratante".

#### **CLÁUSULA NÚMERO \*\*\*: PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal le informamos que los datos personales facilitados, para los casos en que se trate de una persona física, o en el caso de representantes de una persona jurídica, ya sea pública o privada, serán incorporados a un fichero titularidad de la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (en adelante, UNED).

La finalidad de la recogida y tratamiento de la información es la gestión administrativa relativa a la recepción de las ofertas presentadas, así como en su caso, la adjudicación de los correspondientes contratos.

En cumplimiento de la normativa vigente, la UNED garantiza que ha adoptado las medidas técnicas y organizativas necesarias para mantener el nivel de seguridad requerido, en atención a la naturaleza de los datos personales tratados.

Asimismo, la UNED informa que no cederá o comunicará los datos personales almacenados en sus ficheros a terceros, salvo en los supuestos legalmente previstos.

En cualquier momento puede ejercitar los derechos de acceso, rectificación, cancelación u oposición respecto de sus datos personales, enviando un escrito, acompañado de una fotocopia de su DNI, o documento acreditativo equivalente a: UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED). Calle Bravo Murillo, 38. CP 28015 de Madrid.

Para el caso que la contratación implique el acceso, por parte del contratista, a datos de carácter personal de cuyo tratamiento sea responsable la UNED, el primero ostentará la consideración de Encargado del tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre.

En este sentido, los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Disposición Adicional Vigésimo Sexta del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo.

En todo caso, las previsiones del artículo 12.2 de dicha Ley deberán de constar por escrito.

Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que ésta hubiese designado. El tercero Encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

## ANEXO 2.19

Cláusula a insertar en el perfil del contratante de la página Web titularidad de la UNED

En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:

- a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.
- b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.
- c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos el tercero tendrá también la consideración de encargado del tratamiento.

### CURSOS IMPARTIDOS EN LA UNED SOBRE PROTECCIÓN DE DATOS

La finalidad de esta actividad es la de difundir la normativa de Protección de datos y su aplicación en la UNED, mejorando así las buenas prácticas en la institución de la aplicación práctica de esta materia.

1. Curso *Ley de Protección de Datos y su aplicación en la UNED*, en noviembre de 2010, de 18 horas.
2. Curso *Ley de Protección de Datos y su aplicación en la UNED*, en diciembre de 2010, de 18 horas.
3. Curso *Ley de Protección de Datos y su aplicación en la UNED*, en junio de 2011, de 18 horas.
4. Curso sobre la *ley de Protección de Datos y su aplicación en la UNED* celebrado en noviembre y diciembre de 2013, de 25 horas, en la modalidad presencial y on line, 6 horas presenciales y 19 horas on line.
5. Curso Protección de Datos y Nuevas Tecnologías los días 22, 24 y 27 de junio de 2016, de 9 horas de duración, en la modalidad presencial.
6. Curso Protección de Datos y Nuevas Tecnologías los días 17, 19 y 21 de octubre de 2016, de 9 horas de duración en la modalidad presencial.
7. Curso Seguridad y Transparencia en la Gestión de la Información los días 21, 23 y 25 de noviembre de 2016, de 9 horas de duración en la modalidad presencial.
8. Curso Seguridad y Transparencia en la Gestión de la Información los días 14, 16 y 18 de noviembre de 2016, de 9 horas de duración en la modalidad presencial.
9. Curso Seguridad y Transparencia en la Gestión de la Información los días 28 y 30 de noviembre y el 2 de diciembre de 2016, de 9 horas de duración, en la modalidad presencial.
10. Curso Protección de Datos y Nuevas Tecnologías los días 29 de mayo y 1 y 2 de junio de 2017, de 9 horas de duración en la modalidad presencial.

## ASISTENCIA A SEMINARIOS Y JORNADAS DE PROTECCIÓN DE DATOS Y TRANSPARENCIA

Con el fin de implementar en la Universidad la normativa y las nuevas líneas de trabajo de la Agencia Española de Protección de Datos se ha asistido, por parte del personal de la Universidad, a los encuentros y seminarios sobre información y nuevas áreas para innovar en esta materia.

1. Curso sobre *Protección de datos*, impartido por la Agencia Española de Protección de Datos (Septiembre 2006).
2. Encuentro Nacional sobre *Transparencia en la Gestión Universitaria: Protección de Datos y Administración Electrónica* organizado por la Universidad de Burgos (febrero 2008).
3. Asistencia a las *III Jornadas de Protección de Datos en Universidades Públicas de la Comunidad de Madrid*, celebradas en la Universidad Complutense de Madrid el día 7 de mayo de 2008.
4. Asistencia al *V Encuentro entre Agencias Autonómicas de Protección de Datos* celebrado en Madrid en octubre de 2008.
5. Asistencia a la *Segunda Sesión anual abierta de la Agencia Española de Protección de Datos* en enero de 2009.
6. *Tercera Sesión Anual Abierta de la Agencia Española de Protección de Datos* celebrada en octubre de 2010.
7. Seminario sobre *TIC en la Modernización de las Universidades* celebrado en marzo de 2011.
8. *II Jornada Videovigilancia y Protección de Datos* celebrado por la Agencia de Protección de Datos de la Comunidad de Madrid en octubre de 2011.
9. *Congreso Nacional de Interoperabilidad y Seguridad "Una Administración más segura y conectada"* organizado por Club de Innovación en febrero de 2012.
10. Jornada: *Los Archivos Públicos ante la implantación de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno*, organizado por El Instituto Nacional de Administración Pública (INAP) y celebrado el 9 y 10 de diciembre de 2013.
11. Jornada: *Los Archivos Públicos ante la implantación de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno*, organizado por El Instituto Nacional de Administración Pública (INAP) y celebrada el 9 y 10 de diciembre de 2013.

12. Seminario *“Protección de datos y nuevas tecnologías”*, celebrado en Santander del 30 de junio al 4 de julio de 2014.
13. Jornada *“Protección de datos y tratamientos masivos de información”* organizada por la Agencia Española de Protección de Datos en colaboración con la Comisión Europea y celebrada el 28 de enero de 2015 - Día de la Protección de Datos en Europa- con una duración de 5 horas.
14. Séptima Sesión Anual Abierta de la Agencia Española de Protección de Datos (AEPD) el 21 de abril de 2015.
15. Octava Sesión Anual Abierta de la Agencia Española de Protección de Datos (AEPD) el 29 de junio de 2016.
16. Encuentro de E-juristas: Más allá de la Tecnología legal, celebrado en la Universidad Menéndez Pelayo los días 3 y 4 de noviembre de 2006, con una duración de 15 horas.
17. Seminario sobre Datacenter y Ciberseguridad en las AAPP, celebrado en Madrid el 8 de febrero de 2017.

## ANEXO 3.2.

### CURSOS AL PAS DE FORMACIÓN GENERAL, EXTERIOR Y AL PUESTO - PROTECCIÓN DE DATOS

CONVOCATORIA	Nombre del curso	Fecha inicio	Fecha fin	Nº horas	Modalidad	Nº alumnos	EMPRESA/ORGANISMO
401	PROTECCIÓN DE DATOS	18/09/2006	29/09/2006	18	PRESENCIAL	16	AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
423	PROTECCIÓN DE DATOS	02/10/2007	23/10/2007	21	PRESENCIAL	26	AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
433	PROTECCIÓN DE DATOS	20/05/2008	05/06/2008	12	PRESENCIAL	12	UNED
486	LEY DE PROTECCIÓN DE DATOS Y SU APLICACIÓN EN LA UNED	10/12/2010	22/12/2010	18	PRESENCIAL	32	UNED
506	LEY DE PROTECCIÓN DE DATOS Y SU APLICACIÓN EN LA UNED	01/06/2011	13/06/2011	18	PRESENCIAL	18	UNED
573	LEY DE PROTECCIÓN DE DATOS Y SU APLICACIÓN EN LA UNED	04/11/2013	03/12/2013	25	SEMIPRESENCIAL	32	UNED
605	PROTECCIÓN DE DATOS Y NUEVAS TECNOLOGÍAS	23/10/2014	21/11/2014	25	SEMIPRESENCIAL	35	UNED
5404	CONFERENCIA SOBRE EL ADECUACIÓN A LA PROTECCIÓN DE DATOS	16/09/2009	16/09/2009	4	PRESENCIAL	28	AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
10144	JORNADAS SOBRE PROTECCIÓN DE DATOS	21/06/2001	22/06/2001	15	PRESENCIAL	7	UNIVERSIDAD PONTIFICIA COMILLAS
10347	II JORNADAS DE PROTECCIÓN DE DATOS PARA LOS CENTROS PÚBLICOS DE ENSEÑANZA	16/03/2005	16/03/2005	4	PRESENCIAL	2	AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID
10488	TRANSPARENCIA EN LA GESTIÓN UNIVERSITARIA: PROTECCIÓN DE DATOS Y ADMINISTRACIÓN ELECTRÓNICA	14/02/2008	15/02/2008	14	PRESENCIAL	1	UNIVERSIDAD PONTIFICIA COMILLAS
10599	CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD	04/11/2009	05/11/2009	7	PRESENCIAL	2	AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
657	PROTECCIÓN DE DATOS Y NUEVAS TECNOLOGÍAS	22/06/2016	27/06/2016	9	PRESENCIAL	18	UNED
683	PROTECCIÓN DE DATOS Y NUEVAS TECNOLOGÍAS	17/10/2016	21/10/2016	9	PRESENCIAL	23	UNED

## ANEXO 4.1.

### GERENCIA

- **Reglamento sobre Seguridad y buen uso del Sistema de Información de la Universidad Nacional de Educación a Distancia (UNED)**

---

#### Gerencia

- (Aprobado por el Comité de Seguridad de la Información el 22 de noviembre de 2016 y el 14 de julio de 2017).
- (Aprobado en Consejo de Gobierno, celebrado el 12 de diciembre de 2017).

**Reglamento sobre Seguridad y buen uso del Sistema de Información  
de la Universidad Nacional de Educación a Distancia (UNED)**

- (Aprobado por el Comité de Seguridad de la Información el 22 de noviembre de 2016 y el 14 de julio de 2017)
- (Aprobado en Consejo de Gobierno, celebrado el 12 de diciembre de 2017)

**ÍNDICE**

<b>PREÁMBULO</b>	<b>3</b>
<b>TÍTULO PRELIMINAR. Objeto y ámbito de aplicación</b>	<b>4</b>
• Artículo 1. <i>Objeto del Reglamento</i>	4
• Artículo 2. <i>Ámbito de aplicación</i>	4
<b>TÍTULO I. Uso de los Sistemas de Información</b>	<b>4</b>
• Artículo 3. <i>Uso de los Sistemas de Información</i>	4
• Artículo 4. <i>Uso de los equipos informáticos y cualquier otro dispositivo</i>	4
• Artículo 5. <i>Uso de la red corporativa</i>	5
• Artículo 6. <i>Uso de la Información</i>	6
<b>TÍTULO II. Control de accesos</b>	<b>7</b>
• Artículo 7. <i>Acceso a aplicaciones y servicios</i>	7
• Artículo 8. <i>Datos de carácter personal</i>	7
<b>TÍTULO III. Incidencias de seguridad de la Información</b>	<b>7</b>
• Artículo 9. <i>Incidencias de seguridad de ficheros automatizados</i>	7
• Artículo 10. <i>Incidencias de seguridad de ficheros no automatizados o en papel</i>	8
• Artículo 11. <i>Comunicación de incidencias que afecten a la seguridad del Sistema de Información</i>	8
<b>Disposición final primera. Incumplimiento del Reglamento</b>	<b>8</b>
<b>Disposición final segunda. Entrada en vigor</b>	<b>8</b>

## PREÁMBULO

La seguridad de la Información constituye uno de los valores fundamentales en la gestión de cualquier organización. Su aplicación no es sencilla, porque abarca a todos los eslabones de la cadena de gestión de la información y requiere un gran conjunto de medidas organizativas y tecnológicas.

En la sociedad de nuestros días vivimos en un universo digital de información y de datos. La proliferación de ordenadores, teléfonos inteligentes y la vertiginosa evolución de Internet han tenido como consecuencia una expansión, sin precedentes, de la información y de los datos de carácter personal que se gestionan. La Universidad del siglo XXI, por tanto la UNED, tiene que afrontar este hecho, especialmente porque posee una de las bases de datos personales más importantes del país, la de los estudiantes que a lo largo de su historia han pasado por esta institución.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante RLOPD), imponen la obligación a las empresas y organismos, tanto públicos como privados, de establecer unas medidas de seguridad destinadas a garantizar la protección de los datos de carácter personal contenidos en ficheros automatizados o en formato papel.

El Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad (en adelante ENS), modificado por el RD 951/2015, de 23 de octubre, tiene por finalidad la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, señala en su artículo 13.h que uno de los derechos de las personas en sus relaciones con las Administraciones Públicas es: *“la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas”*.

Del mismo modo, en su artículo 17.3 “Archivo de documentos” dispone que: *“Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos”*

Por ello, conocer el Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED, es uno de los pilares de la gestión de calidad de nuestra Universidad.

**TÍTULO PRELIMINAR****Objeto y ámbito de aplicación*****Artículo 1. Objeto del Reglamento.***

La UNED tiene entre sus objetivos garantizar la seguridad de los Sistemas de Información, mediante la implantación del ENS, así como garantizar la protección de los datos de carácter personal de todas aquellas personas que con ella se relacionan: estudiantes, profesores, personal de administración y servicios y, en general, cualquier otro ciudadano que en algún momento de su vida tenga relación con nuestra institución, poniendo los medios necesarios para llevar a cabo las medidas de índole técnico y organizativo que permitan un adecuado tratamiento de estos datos en la Universidad.

Uno de los eslabones, normalmente, más débil es precisamente el usuario final del sistema (tanto en el uso de la informática como en soporte papel).

Por tanto, éste necesita ser consciente de las situaciones de riesgo en materia de seguridad de la información y, al mismo tiempo, debe disponer de unas normas respecto al uso correcto de los sistemas informáticos a su alcance, así como de los soportes o documentos en papel y, con especial relevancia, deberá preservar la confidencialidad de la información de carácter personal que esté siendo tratada.

El éxito de su implantación depende, además, de que exista en todos los niveles una cultura de la seguridad, es decir, una concienciación sobre la necesidad de que la información se mantenga en secreto, íntegra y disponible.

En consecuencia el presente documento fija las pautas de seguridad del uso del ordenador asignado al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, tanto en soporte informático como en papel.

***Artículo 2. Ámbito de aplicación.***

Este Reglamento será de aplicación a todos los miembros de la comunidad universitaria que utilicen los recursos informáticos de la universidad, bien sea de forma local o remota y accedan o traten información de carácter personal en soporte informático o en papel, para la realización de sus funciones.

Así mismo, se aplicará a cualquier otra persona o entidad externa que utilice o acceda a los recursos informáticos de la Universidad al prestar servicios a la misma.

**TÍTULO I****Uso de los Sistemas de Información*****Artículo 3. Uso de los Sistemas de Información.***

Los datos, dispositivos, programas y equipos informáticos que la Universidad pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones y fines previstos, debiendo constituir una herramienta de trabajo o estudio y no deben ser utilizados para fines privados.

***Artículo 4. Uso de los equipos informáticos y cualquier otro dispositivo de acceso a la información.***

La política de seguridad de la información comportará el cumplimiento por parte de los usuarios de las siguientes obligaciones dirigidas a una utilización responsable de los recursos informáticos.

1. Respetar la configuración física de los equipos no conectando otros dispositivos a iniciativa del usuario, así como no variar su ubicación, excepto cuando las actividades docentes o

investigadoras lo justifiquen. Estas deberán ser acreditadas en caso de producirse alguna incidencia en el Sistema de Información.

2. Mantener la configuración software de los equipos, no desinstalando o instalando programas o cualquier otro tipo de software distinto a la configuración lógica predefinida, excepto cuando las actividades docentes o investigadoras lo justifiquen. Estas deberán ser acreditadas en caso de producirse alguna incidencia en el Sistema de Información.
3. Las contraseñas de acceso al equipo, al sistema y a la red, concedidas por la UNED, son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida.  
De este modo, los usuarios no deberán:
  - a) Emplear identificadores y contraseñas de otros usuarios para acceder al sistema y a la red corporativa.
  - b) Intentar modificar o acceder al registro de accesos.
  - c) Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a los ficheros.
  - d) En general, emplear la red corporativa, sistemas, equipos informáticos y cualquier medio puesto al alcance del usuario, vulnerando el derecho de terceros, los propios de la Institución o, bien, para la realización de actos que pudieran ser considerados ilícitos.
4. No se podrán utilizar archivos o ficheros titularidad de la UNED para uso particular y de terceros. Por ello, no se deberá copiar o enviar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de la Universidad en ordenadores propios, pen drives o cualquier otro soporte informático. En caso de que así fuera necesario, por motivos de trabajo, serán eliminados una vez que hayan dejado de ser útiles para los fines que motivaron su creación. Asimismo, durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte informático de su propiedad, deberá restringir el acceso y uso de la información que obra en los mismos.
5. Se establecerán medidas de protección adicionales que aseguren la confidencialidad y la seguridad de la información almacenada en el equipo cuando el usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.

#### **Artículo 5. Uso de la red corporativa.**

La red corporativa es un recurso compartido y limitado, que sirve no sólo para el acceso de los usuarios internos de la UNED a la Intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas corporativas.

Los usuarios deberán cumplir las siguientes medidas de seguridad establecidas por la UNED:

1. La utilización de Internet por parte de los usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña como personal de la UNED o que pudiera conducir a una mejora en la calidad del trabajo desarrollado. Se debe, por tanto, evitar la utilización que no tenga relación con las funciones del puesto de trabajo del usuario.
2. No está permitido el uso de programas para compartir contenidos, con finalidades distintas a las relacionadas con el puesto de trabajo.
3. El correo electrónico se considera como un instrumento básico de trabajo. El acceso al correo se realizará mediante una identificación consistente en un usuario y una contraseña. Dicha identificación deberá seguir las mismas directrices que las planteadas, para el acceso a las aplicaciones, en el artículo 7 de este Reglamento.
4. Los envíos masivos de información así como los correos que se destinen a gran número de usuarios, serán sólo los estrictamente necesarios.
5. Se evitará abrir anexos de mensajes, ficheros sospechosos o de procedencia desconocida.

6. La UNED podrá adoptar las medidas oportunas para asegurar el uso apropiado de los recursos telemáticos disponibles, con el fin de garantizar el servicio público encomendado.

**Artículo 6. Uso de la información.**

La información contenida en los Sistemas de Información de la UNED es propiedad de la misma.

Los usuarios deben conocer y cumplir las normas de uso que se enumeran a continuación:

1. La información contenida en los Sistemas de Información o que circule por sus redes de comunicaciones debe ser utilizada exclusivamente para el cumplimiento de las funciones profesionales o académicas del usuario.
2. Los usuarios sólo podrán acceder a aquella información para la que posean autorización, concedida por el Centro de Tecnología de la UNED (CTU), en función del colectivo al que pertenezcan, manteniendo absoluta reserva sobre la misma.
3. Se evitará almacenar información sensible, confidencial o protegida en soportes tales como CDs, DVDs, memorias USB, pen drives, listados, etc., o dejar visible tal información en la pantalla del ordenador.
4. En el caso de envíos de documentación en soporte papel, que contengan datos sensibles, se deberán realizar bien en sobre cerrado si se tratase de correo interno dentro de la Universidad, o bien, por correo certificado o a través de correo ordinario que permita su completa confidencialidad, para envíos fuera de la Universidad.
5. La información se deberá almacenar en el espacio de la red informática habilitado por la UNED, a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas. En el caso de los documentos en papel, se guardarán en un lugar seguro impidiendo que un tercero no autorizado pueda tener acceso.
6. Se evitará almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento de la red compartida de la UNED.
7. Los usuarios no deberán abandonar documentos que contengan datos personales en faxes, impresoras, escáneres, u otra maquinaria. Asimismo no se dejará documentación visible en los escritorios, mostradores u otro mobiliario.
8. En el caso de que deban transmitirse datos sensibles, confidenciales o protegidos, se cifrarán o se utilizará cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte.
9. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser destruidos, preferentemente, mediante máquinas destructoras de papel o por el procedimiento utilizado por la empresa adjudicataria de este servicio, de forma que no sea recuperable la información que pudieran contener.
10. En el caso de dar de baja dispositivos hardware, que contengan datos de carácter personal, el usuario deberá solicitar al Centro de Atención al Usuario (CAU) el borrado seguro de datos, que el técnico, autorizado por el usuario y con el Vº Bº del responsable de la unidad, realizará mediante un proceso de formateo a bajo nivel del disco duro.
11. Se comunicarán, al responsable del fichero, las entradas y salidas de la información contenida en dispositivos móviles (portátiles, teléfonos, Tablet) o soportes como memorias USB, CDs, DVDs, etc., así como en soporte papel, fuera de las instalaciones de la UNED.
12. Los ficheros temporales, creados para el desarrollo de una tarea determinada, deberán ser borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación y mientras estén vigentes deberán almacenarse en la carpeta habilitada en la red informática. Si transcurrido un mes, el usuario detecta la necesidad de seguir utilizando la información deberá comunicarlo al responsable de seguridad, para adoptar las medidas oportunas.

## TÍTULO II

### Control de accesos

#### **Artículo 7. Acceso a aplicaciones y servicios.**

Gran parte de los procedimientos administrativos se gestionan en la actualidad accediendo desde ordenadores personales a aplicaciones que residen en servidores conectados a la red corporativa. El acceso se realizará previa identificación, mediante las claves de usuario y contraseña proporcionadas a los usuarios y, por ello, deberán cumplir con las siguientes medidas de seguridad establecidas por la UNED:

1. La custodia de la contraseña es responsabilidad del usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona.
2. Las contraseñas no deben anotarse, deben recordarse.
3. Las contraseñas deben cambiarse periódicamente y en ningún caso será superior a un año. Los usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo crean conveniente.
4. Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al responsable de seguridad.
5. Al abandonar el puesto de trabajo deben cerrarse las sesiones con las aplicaciones establecidas y apagar los equipos al finalizar la jornada laboral, excepto en los casos en que el equipo deba permanecer encendido.

#### **Artículo 8. Datos de carácter personal.**

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, se obliga al cumplimiento de la Ley Orgánica 15/1999, de 13 de octubre (BOE del 14), de Protección de Datos de Carácter Personal (en adelante, LOPD); y del Real Decreto 1720/2007, de 21 de diciembre (BOE del 19 de enero de 2008), por el que se aprueba el Reglamento de desarrollo de la LOPD.

Dichos deberes del usuario incluyen el deber de secreto de los datos de carácter personal y la custodia de los mismos; el deber de seguridad de los datos para evitar su alteración, pérdida, tratamiento o acceso no autorizado, el deber de no comunicación de los datos de carácter personal objeto de tratamiento a un tercero, salvo para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con previo consentimiento del interesado.

## TÍTULO III

### Incidencias de seguridad de la Información

#### **Artículo 9. Incidencias de seguridad de ficheros automatizados.**

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

Entre otros, tienen la consideración de incidencias de seguridad que afectan a los ficheros automatizados, los supuestos siguientes:

1. La pérdida de contraseñas de acceso a los Sistemas de Información
2. El uso indebido de contraseñas
3. El acceso no autorizado de usuarios a ficheros, sin el perfil correspondiente
4. La pérdida de soportes informáticos con datos de carácter personal
5. La pérdida de información por el mal uso de las aplicaciones
6. Ataques a la red
7. Infección de los sistemas de información por virus u otros elementos dañinos
8. Fallo o caída de los Sistemas de Información

**Artículo 10. Incidencias de seguridad de ficheros en papel.**

Tienen la consideración de incidencias de seguridad, que afectan a los ficheros en papel, las siguientes:

1. La pérdida de las llaves de acceso a los archivos, armarios y dependencias, donde se almacena la información
2. El uso indebido de las llaves de acceso
3. El acceso no autorizado de usuarios a los archivos, armarios y dependencias, donde se encuentra archivada la información
4. La pérdida de soportes o documentos en papel
5. El deterioro de los soportes o documentos, armarios y archivos, donde se encuentra guardada la información

**Artículo 11. Comunicación de las incidencias que afecten a la seguridad del Sistema de Información.**

1. Una vez producida la incidencia, el usuario conocedor de la misma, debe comunicarla al Centro de Atención al Usuario (CAU) telefónicamente o a través de las direcciones: [soportePAS@csi.uned.es](mailto:soportePAS@csi.uned.es) o [soportePDI@csi.uned.es](mailto:soportePDI@csi.uned.es)
2. Informará al Responsable del fichero o en su defecto al Responsable directo de su Unidad.
3. En el caso de que se hayan visto afectados ficheros con datos de carácter personal de nivel medio o alto y sea necesario llevar a cabo algún procedimiento de recuperación de datos, será imprescindible que el Responsable del fichero autorice la ejecución del citado procedimiento. Para ello el CAU deberá requerir al usuario la citada autorización.
4. El personal del CAU tomará las medidas oportunas para que, en el menor tiempo posible, se subsane la anomalía que haya generado la incidencia.
5. El CAU remitirá, mensualmente, al Departamento de Política Jurídica de Seguridad de la Información un informe con las incidencias producidas y que afecten a la pérdida de información o de datos de carácter personal, a la dirección de correo electrónico: [dptojuridicoseguridad@adm.uned.es](mailto:dptojuridicoseguridad@adm.uned.es), para su registro en el Documento de Seguridad.

**Disposición final primera. Incumplimiento del Reglamento.**

Todos los usuarios de la UNED están obligados a cumplir lo prescrito en el presente Reglamento sobre Seguridad y buen uso del Sistema de Información.

El incumplimiento de este Reglamento y los posibles incidentes que puedan derivarse, serán responsabilidad del usuario, así como las implicaciones legales correspondientes.

**Disposición final segunda. Entrada en vigor.**

El Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED entrará en vigor al día siguiente de su publicación en el BICI.

ANEXO 4.2.

# Normativa de uso del correo electrónico de la UNED



(Aprobado por el Comité de Seguridad de la Información el 22 de noviembre de 2016)

## ÍNDICE

1. OBJETIVO Y ÁMBITO DE APLICACIÓN.....	3
2. ACCESO A LOS SERVICIOS .....	3
3. RESPONSABILIDADES DEL USUARIO .....	3
4. USOS INCORRECTOS DE LOS SERVICIOS .....	6

## **1. OBJETIVO Y ÁMBITO DE APLICACIÓN**

La Universidad Nacional de Educación a Distancia (UNED) ofrece a la comunidad universitaria el servicio de Correo Electrónico. El objetivo de esta Normativa de Uso es garantizar la calidad del mismo y un uso de acuerdo con los fines últimos de la Universidad.

Otros objetivos que persigue esta normativa son los siguientes:

- a) Preservar la privacidad y seguridad de las comunicaciones de la UNED
- b) Evitar situaciones que puedan causar algún tipo de responsabilidad civil o penal
- c) Garantizar la seguridad y el rendimiento de los sistemas informáticos de la UNED

**Los usuarios del servicio** están obligados al cumplimiento de la normativa redactada en el presente documento.

## **2. ACCESO A LOS SERVICIOS**

### **2.1.- Usuarios de los servicios**

Pueden disfrutar del servicio de correo electrónico de la UNED los miembros de la comunidad universitaria, tanto los estudiantes matriculados, como el personal docente e investigador y el personal de administración y servicios, además de las entidades o personas autorizadas en virtud del convenio o autorización emitida por el órgano competente de la UNED.

El servicio se relaciona a la existencia del vínculo con la Universidad.

## **3. RESPONSABILIDADES DEL USUARIO**

### **3.1.- Aceptación de las condiciones y normas de uso**

La utilización del servicio de Correo Electrónico proporcionado por la UNED implica el conocimiento y plena aceptación de las normas de uso y condiciones que se especifican en el presente documento y otras normativas legales que puedan ser de aplicación.

### **3.2.- Identificación y autenticación de los usuarios**

Las credenciales de acceso al servicio del correo electrónico (identificador de usuario y contraseña) son de uso personal e intransferible. El usuario es responsable de cualquier uso ilícito de dichas credenciales y de las consecuencias que del uso indebido de la misma se puedan derivar.

En relación a las claves de acceso (contraseñas) al servicio de usuarios se tendrán en cuenta las siguientes consideraciones:

- a) Utilizar claves de acceso seguras (longitud, caracteres especiales, etc.)
- b) Proceder al cambio de clave al menos una vez al año o cuando existan indicios de que es conocida por un tercero
- c) Establecer claves de acceso que limiten la entrada al correo electrónico desde dispositivos móviles (Smartphone, Tablet, etc.)

### **3.3.- Confidencialidad del correo electrónico**

La utilización del correo electrónico como medio para la transmisión de datos personales considerados como especialmente protegidos – datos relativos a salud, ideología, afiliación sindical, religión y creencias, orientación sexual, origen racial – solo podrá realizarse adoptando mecanismos de cifrado u otros equivalentes que garanticen que la información sea ininteligible por personas no autorizadas.

### **3.4.- Uso exclusivo del correo electrónico para comunicaciones interpersonales**

El correo electrónico es una herramienta para el intercambio de información entre personas, no un medio de difusión masiva e indiscriminada de información. Para ello existen otros canales más adecuados y efectivos.

### **3.5.- Uso para fines profesionales o académicos**

Las cuentas de correo de la UNED no deben ser utilizadas para fines privados, ya que constituyen una herramienta de trabajo. **Para los fines profesionales o académicos, únicamente se podrán utilizar las cuentas de correo corporativo.**

### **3.6.- Utilización de copia oculta en el envío de correos electrónicos**

La normativa de Protección de Datos establece que las direcciones de correo electrónico constituyen un dato de carácter personal. Por este motivo su tratamiento debe tener, por regla general, el carácter de confidencial y secreto.

En el supuesto de introducir las direcciones de correo electrónico para su envío a terceras personas, en una comunicación múltiple, es preciso insertarlas en el campo “CCO” (copia carbón oculta) para no incurrir así en una vulneración de lo dispuesto en el artículo 10 de la Ley Orgánica de protección de Datos de Carácter Personal, por incumplir con el deber de secreto y confidencialidad de los datos. De esta forma la lista de los contactos del correo electrónico no será visible para quien lo reciba.

En los grupos de trabajo que se considere de interés conocer qué personal de la Universidad es destinatario de una comunicación múltiple no se infringe la normativa de protección de datos.

### **3.7.- Texto legal en la firma del correo electrónico**

Se recomienda incluir en todos los correos electrónicos el texto legal que indique al destinatario aquellos aspectos legales a los que puedan estar sujetos los correos remitidos.

Se recomienda la inclusión, por defecto, del siguiente texto legal:

**AVISO LEGAL.** Este mensaje puede contener información reservada y confidencial destinada exclusivamente al destinatario. Si usted no es el destinatario no está autorizado a copiar, reproducir o distribuir este mensaje ni su contenido. Si ha recibido este mensaje por error, le rogamos que lo notifique al remitente.

Le informamos de que sus datos personales, que puedan constar en este mensaje, están incorporados a un fichero titularidad de la UNED cuya finalidad es la de mantener el contacto con usted. En cualquier momento podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición ante la UNED, [Departamento de Política Jurídica de Seguridad de la Información](#), o a través de la [Sede electrónica](#) de la Universidad.

### **3.8.- Correo no deseado (SPAM)**

El usuario no deberá contestar aquellos correos no deseados (SPAM), ni descargar ningún archivo adjunto, ni acceder a ningún enlace que aparezca en el cuerpo del correo. El responder o acceder a alguno de los enlaces incluidos en este tipo de correos, puede incrementar el número de correos no deseados recibidos al confirmar que la cuenta está activa.

El usuario no deberá aceptar documentos ni archivos adjuntos que provengan de desconocidos o que tengan un origen poco fiable. Será necesario, **tener precaución** para determinar qué correos pueden suponer una amenaza tanto para el servicio de correo electrónico como para el equipo del usuario en el que se descarga el documento o archivo adjunto.

### **3.9. Incidencias del servicio**

El usuario tiene la obligación de poner en conocimiento del Responsable correspondiente, el uso indebido o no autorizado de su cuenta de correo electrónico a la mayor brevedad posible, así como cualquier otra incidencia relacionada con el funcionamiento del servicio a través de la dirección de correo: [admin.correo@csi.uned.es](mailto:admin.correo@csi.uned.es)

#### **4. USOS INCORRECTOS DE LOS SERVICIOS**

Se considera incumplimiento de las condiciones y normas de uso del correo electrónico de la UNED, los supuestos siguientes:

- a) Difusión de contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentar contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
- b) Difusión de mensajes de correo electrónico sin identificar plenamente a su remitente.
- c) Difusión de mensajes comerciales o propagandísticos sin autorización expresa.
- d) Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.
- e) Envío masivo de mensajes o información que consuma injustificadamente recursos de la UNED.

## **ANEXO 4.3.**

# **Procedimiento de desechado y destrucción de documentos con datos de carácter personal en papel, de la UNED**

**(Aprobado por el Comité de Seguridad de la Información el 22 de noviembre de 2016)**

## ÍNDICE

1.- OBJETO.....	3
2.- ALCANCE .....	3
3.- DESCRIPCIÓN DEL PROCEDIMIENTO.....	3
3.1.- Introducción.....	3
3.2.- Comunicación del desechado de documentos por los usuarios.....	4
3.3.- Actuación del Responsable del Fichero ante la solicitud de destrucción de un Fichero “íntegro” por un usuario .....	4
3.4.- Actuación del Responsable de Seguridad ante la solicitud de destrucción de un Fichero “íntegro” por el Responsable del Fichero .....	4
3.5.- Medidas de seguridad a adoptar en el desechado o destrucción de documentos.....	5
4.- NORMATIVA .....	6
5.- FUNCIONES Y RESPONSABILIDADES .....	7
Responsable del Fichero .....	7
Responsable de Seguridad.....	7
Gestor de Fichero .....	8
Usuario .....	8
6.- CONTRATACIÓN DE EMPRESAS ESPECIALIZADAS .....	8
ANEXO I: DEFINICIONES.....	9
ANEXO II: SOLICITUD DE SUPRESIÓN DE FICHERO.....	11

## **1.- OBJETO**

Establecer el método para el desechado y destrucción de documentos con datos de carácter personal por los usuarios.

## **2.- ALCANCE**

El procedimiento es aplicable al desechado y destrucción de documentos con datos de carácter personal que se produzcan en la UNED.

El REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RLOPD), obliga a la adopción de determinadas medidas para garantizar la seguridad de los datos en soporte papel, en el caso de que sea desechado o destruido.

## **3.- DESCRIPCIÓN DEL PROCEDIMIENTO**

### **3.1.- Introducción**

El fomento de la seguridad de la información y la exigente normativa en cuanto a la destrucción de la información desechada cobran cada vez más importancia. De esta forma se debe concienciar al personal de la Universidad a adoptar los procesos que aseguren el cumplimiento de las normas establecidas.

La información manejada por la UNED es considerada como uno de sus activos fundamentales y, en consecuencia, debe ser protegida como tal hasta el mismo instante de su destrucción. Dichos activos son desechados a diario y son gestionados por servicios de limpieza de oficinas, por empresas de reciclaje de papel, en pequeñas destructoras, o bien se contrata a una empresa externa para su destrucción. En todos los casos hay que definir protocolos de actuación que garanticen la gestión confidencial y la no recuperación de los documentos.

El artículo 92.4 del RLOPD indica sobre la “Gestión de soportes y documentos” que:

*“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”.*

Asimismo, el artículo 112 del RLOPD, referente a la “Copia o reproducción de documentos” dispone lo siguiente:

- 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.*

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.*

El cumplimiento de esta legislación es transversal por lo que afecta a todas las áreas y no depende sólo y exclusivamente de un Departamento.

### **3.2.- Comunicación del desechado de documentos por los usuarios**

1. El usuario que elimine todos los documentos integrantes de un fichero, ha de comunicarlo al Responsable del Fichero o al Gestor de Fichero correspondiente.
2. En el supuesto de que no lo comunicase, podría incurrir en una falta contra la seguridad de la información.

Los usuarios no procederán a la destrucción o desechado de ningún fichero “íntegro” sin la autorización del Responsable del Fichero.

### **3.3.- Actuación del Responsable del Fichero ante la solicitud de destrucción de un Fichero “íntegro” por un usuario**

1. Una vez recibida la solicitud, el Responsable del Fichero comprobará si se debe o no efectuar la destrucción (teniendo en cuenta la distinta normativa vigente, aplicable en temas de conservación de la información para los distintos ficheros tratados). Si es así, el Responsable del Fichero lo comunicará al Responsable de Seguridad.

*En ningún caso se podrá autorizar la eliminación de un fichero físico en papel ni se podrá proceder a la destrucción de documentos en tanto subsista el valor probatorio de los derechos y obligaciones de las personas físicas o jurídicas o no hayan transcurrido los plazos que la legislación vigente establezca para su conservación.*

2. El Responsable del Fichero adoptará las medidas necesarias para garantizar que el usuario procede a la destrucción física del fichero y evitar así el acceso a la información contenida o su recuperación posterior.

### **3.4.- Actuación del Responsable de Seguridad ante la solicitud de destrucción de un Fichero “íntegro” por el Responsable del Fichero**

1. Recibida la solicitud (Anexo II), se valorará el alcance que supone la destrucción del fichero.
  - a) Si el fichero jurídico asociado estaba registrado como “no automatizado o en papel”, deberá notificar a la AEPD la supresión del mismo.

b) Si el fichero jurídico asociado estaba registrado como “mixto”, deberá comunicar a la AEPD la modificación del fichero de forma que aparezca como fichero “automatizado”.

2. El Responsable de Seguridad deberá actualizar en el Documento de Seguridad todos los cambios que se deriven de la modificación o supresión del fichero.

### 3.5.- Medidas de seguridad a adoptar en el desechado o destrucción de documentos

Conservar cierto tipo de información más allá del tiempo estrictamente necesario, además de generar numerosos costes de almacenamiento puede suponer una serie de problemas.

La normativa europea relativa a la protección de datos exige una serie de niveles de seguridad en la destrucción de documentos. Para ello toda organización debe definir los objetivos y desarrollar un procedimiento en la supresión de la documentación con la que cuenta. Todo ello de forma segura y cerciorándose de la imposibilidad de cualquier posible reconstrucción.

Por lo tanto, cuando por su propia naturaleza, o por haber agotado el ciclo de vida útil, el soporte/documento deba ser desechado, y por tanto, destruido, se adoptarán las siguientes precauciones:

1. **No tirar** documentos en papel que contengan datos personales a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información.
2. En caso de **desechar un documento** que contenga datos de carácter personal, se procederá a su destrucción utilizando una **destructora** de papel. Otros métodos no garantizan la total destrucción de documentos y, por tanto, la imposibilidad de que alguien recupere su contenido.



Si se trata de destruir un gran número de documentos, se deberá remitir un correo electrónico al Departamento de Servicios Generales solicitándolo. Este Departamento se encargará de su retirada, destrucción (certificada) y posterior reciclaje.

3. **Los ficheros temporales o copias de trabajo de documentos**, cuando hayan dejado de ser necesarios para los fines que motivaron su creación, serán destruidos.
4. No se aconseja en ningún caso **la reutilización de documentos de papel impreso a una cara** ya que resulta ineficiente y peligroso desde el punto de vista de la seguridad.
5. Los documentos que van a ser eliminados **deben de estar protegidos hasta el momento de su destrucción física**. El lugar o los contenedores donde se almacenen requieren medidas de seguridad eficaces frente a posibles accesos por parte de un tercero. No deben permanecer al descubierto en el exterior de los edificios. Tampoco deben amontonarse en lugares de paso ni en locales abiertos. Se deben guardar en locales o contenedores con mecanismos de cierre, garantizando así su seguridad.
6. El método más adecuado para la destrucción de documentos es la **trituration** mediante corte en tiras o cruzado. Es conveniente, en ciertos casos, la adquisición de una destructora de papel que en el momento actual tienen un coste bajo. El papel se hace tiras o partículas, cuyo tamaño se elegirá en relación al nivel de protección requerido por la información contenida en los documentos a destruir.

#### 4.- NORMATIVA

- ✓ **LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)**
- ✓ **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 (RLOPD)**
- ✓ **DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo relativo al tratamiento de datos personales y a la libre circulación de estos datos. (En vigor hasta el 24 de mayo de 2018)**
- ✓ **REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Será aplicable a partir del 25 de mayo de 2016**
- ✓ **NORMATIVA PROPIA DEL ARCHIVO GENERAL DE LA UNED**

## **5.-FUNCIONES Y RESPONSABILIDADES**

### **Responsable del Fichero**

El Responsable del Fichero tendrá las siguientes funciones:

1. Notificar al Responsable de Seguridad la supresión, modificación o alta de ficheros con nivel de seguridad medio o alto.
2. Dirigir y coordinar las funciones del personal que esté a su cargo, con el fin de que se garantice el nivel de protección de los datos de carácter personal.
3. Mantener el correcto estado de los armarios, archivos y dependencias que contienen los ficheros, en cuanto a la seguridad y privacidad de la información de carácter personal que se encuentre en ellos.
4. Establecer los permisos de los usuarios con acceso autorizado a los armarios, archivos y dependencias citados.
5. Estipular el procedimiento de archivo de los documentos de acuerdo con criterios que garanticen la correcta conservación de los mismos, la localización, la consulta de la información y la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
6. Cuidar de que los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal dispongan de mecanismos que obstaculicen su apertura como, por ejemplo, llaves. Si las características físicas de aquéllos no permiten adoptar esta medida, el Responsable del Fichero adoptará aquellas que impidan el acceso de personas no autorizadas.
7. Mantener informado al usuario para efectuar una entrada o salida de archivos en papel.

### **Responsable de Seguridad**

El Responsable de Seguridad es competente para llevar a cabo las siguientes funciones:

1. Funciones de control relativas a garantizar el cumplimiento de las medidas de seguridad que detalla el RLOPD para ficheros no automatizados (en papel).
2. Actuaciones relativas a las medidas que garanticen el cumplimiento de las obligaciones jurídicas.

3. Notificar a la Agencia Española de Protección de Datos la supresión, modificación o alta de ficheros a los que se les aplicarán las medidas de seguridad de nivel medio o alto según el RLOPD.

### **Gestor de Fichero**

1. Sus funciones y obligaciones son las mismas que las del Responsable del Fichero delegadas por éste, como actividades de control y ejecución de medidas de seguridad relacionadas con ficheros “concretos”, a excepción de la notificación de la creación, supresión o modificación de ficheros que correrá a cargo, en este caso, del Responsable del Fichero.

### **Usuario**

1. Notificar al Responsable del Fichero el desechado de un fichero físico en papel cuando se realice íntegramente.
2. Cumplir con las obligaciones respecto al tratamiento, manipulación, reutilización o desechado de los ficheros en papel con datos de carácter personal.

## **6.- CONTRATACIÓN DE EMPRESAS ESPECIALIZADAS**

Cuando se acuda a un tercero para la destrucción de documentos se deberá celebrar un contrato de acceso a datos por cuenta de terceros y aquél deberá certificar la efectiva destrucción de los soportes.

Al contratar este servicio es importante asegurarse de que la empresa puede comprometerse a:

- ✓ Garantizar la destrucción de los documentos en sus instalaciones y con medios propios sin subcontratos que comporten el manejo de los mismos por parte de otras empresas sin conocimiento del responsable de los documentos.
- ✓ Permitir que, siempre que se estime conveniente, un representante del responsable de los documentos presencie su destrucción y compruebe las condiciones, en que se realiza.
- ✓ Certificar la destrucción de los documentos dejando constancia del momento y de la forma de destrucción.

## ANEXO I

### DEFINICIONES

#### **Datos de carácter personal.**

Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

#### **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 desproporcionados.

#### **Fichero de datos de carácter personal**

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.

#### **Fichero no automatizado o en papel**

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 personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

#### **Soporte físico de almacenamiento-papel**

Objeto físico que almacena o contiene datos o documentos.

Ejemplos de soporte de almacenamiento-papel: archivadores, estanterías, armarios... que almacenen archivos en papel con datos de carácter personal.

#### **Responsable del Fichero o del Tratamiento**

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

### **Responsable de Seguridad**

Persona o personas a las que se ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables al tratamiento no automatizado (en papel) de los datos de carácter personal. En la UNED desempeñan estas funciones:

La Jefa de la Sección de Protección de Datos

### **Gestor de Fichero**

El Gestor de Fichero es una figura que se ubica en una situación intermedia entre el Responsable del Fichero y los usuarios del sistema. Se delegan actividades de control y ejecución de medidas de seguridad relacionadas con ficheros “concretos”. Esto permite una adecuada colaboración con las tareas del Responsable debido a su relación directa con el fichero y a su cercanía con los usuarios.

### **Usuario**

Sujeto autorizado para acceder y tratar los datos de carácter personal, en soporte informático y en papel.

**ANEXO II**

**SOLICITUD DE SUPRESIÓN DE FICHERO ÍNTEGRO**

**DATOS DE LA PERSONA INTERESADA**

D/D<sup>a</sup> , cargo o  
puesto de trabajo , teléfono  
, e-mail , por medio del presente escrito

**SOLICITA,**

La **supresión** del fichero denominado  y que se  
inicien los trámites previstos en el art. 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de  
Protección de Datos de Carácter Personal, y en el artículo 52 del Real Decreto 1720/2007, de 21  
de diciembre, por el que se desarrolla la mencionada norma.

El motivo o causa de la **supresión** sería

En caso de producirse la supresión del fichero, el **destino** de la información contenida en  
él sería

a  de  de 20

**Firma de la persona solicitante**

Remitir a la dirección: [incidenciaslopd@adm.uned.es](mailto:incidenciaslopd@adm.uned.es)

ANEXO 4.4.

# **PROCEDIMIENTO PARA DAR DE BAJA DISPOSITIVOS HARDWARE**

**(Aprobado por el Comité de Seguridad de la Información el 10 de mayo de 2017)**

## ÍNDICE

1. OBJETO.....	3
2. ÁMBITO.....	3
3. PROCEDIMIENTO DE BAJA DE DISPOSITIVOS HARDWARE.....	3
4. AUTORIZACIÓN DEL BORRADO SEGURO .....	4

## 1. OBJETO

El presente documento tiene por objeto describir el proceso de baja y retirada de los dispositivos hardware de los distintos puestos de trabajo de la Universidad, pudiendo ser reutilizados aquellos que no se consideren obsoletos.

## 2. ÁMBITO

Este procedimiento se aplica al personal de la UNED (PDI y PAS) que solicite dar de baja dispositivos hardware: impresora, escáner, aparato multifunción, monitor, CPU, portátil, servidores y equipamiento similar.

## 3. PROCEDIMIENTO DE BAJA DE DISPOSITIVOS HARDWARE

### 3.1. Baja y retirada de un equipo, salvo las CPU, dispositivos de almacenamiento, portátiles y servidores:

**3.1.1.** El usuario debe cumplimentar el formulario del modelo 27 “SOLICITUD DE BAJA DE EQUIPOS INFORMÁTICOS (HARDWARE) DE LA UNED” con los datos del componente hardware. Este formulario lo puede obtener en el Portal UNED estando autenticado y la ruta a seguir es la siguiente:

**LA UNED > INSTITUCIONAL > GERENCIA > PROCEDIMIENTOS PRESUPUESTARIOS Y MODELOS > MODELOS**

**3.1.2.** Una vez cumplimentado debe enviarlo al Departamento de Infraestructura mediante correo electrónico.

### 3.2. Baja y retirada de las CPU, dispositivos de almacenamiento, portátiles y servidores:

**3.2.1.** El usuario debe cumplimentar el formulario del modelo 27 “SOLICITUD DE BAJA DE EQUIPOS INFORMÁTICOS (HARDWARE) DE LA UNED”.

**3.2.2.** Solicitará al CAU **el borrado seguro de datos** del equipo que se quiere dar de baja, a través de la Autorización del modelo 27: “Autorización del borrado seguro de datos para realizar la baja del equipo”. Deberá firmar el usuario, con el visto bueno del Responsable de la Unidad, así como el técnico que proceda al formateo del equipo, por duplicado, valorando la posible reutilización del dispositivo. Una copia se archivará en el CAU y la otra se enviará al Departamento de Infraestructura, donde se actualizará el inventario del dispositivo.

**3.2.3.** Cuando los datos que hay almacenados en el disco duro sean confidenciales o especialmente protegidos, el técnico tendrá que utilizar el software especial para borrado seguro de datos.

## Autorización del borrado seguro de datos para realizar la baja del equipo

Núm. Inventario \_\_\_\_\_

Núm. Incidencia: \_\_\_\_\_

Fecha: \_\_\_\_\_

Autorizo al técnico informático a realizar el borrado seguro de los datos del disco duro, conociendo que este proceso **BORRARÁ DEFINITIVAMENTE** los datos contenidos en él y que serán **IRRECUPERABLES**. Asimismo, autorizo, en su caso, a que el técnico retire el equipo para realizar este proceso.

Datos del usuario del equipo	Técnico que realiza el servicio
_____ _____	_____ _____
Fdo:	Fdo:
Vº Bº Responsable de la Unidad	

**ANEXO 4.5.**

**Procedimiento de actuación ante la baja definitiva del usuario del Sistema Información UNED**

**Centro de Tecnología de la UNED**

**(Aprobado por el Comité de Seguridad de la Información el 19 de mayo de 2015)**

Código: CTU-AU-PGS-BAJUSR

Fecha en vigor: N° de Páginas: 5

# ÍNDICE

1 OBJETO.....	3
2 ÁMBITO.....	3
3 CONTENIDO .....	3
4 ANEXO 1 .....	4
5 ANEXO 2 .....	5

## **OBJETO**

El objetivo de este procedimiento es la utilización y el destino del equipo informático, propiedad de la UNED, que ha venido utilizando un usuario que causa baja definitiva por cualquier circunstancia.

## **ÁMBITO**

Este procedimiento se aplicará en las bajas de los usuarios del Sistema de Información de la UNED.

## **CONTENIDO**

Los equipos informáticos son propiedad de la UNED, que los cede a sus trabajadores para que puedan desarrollar su actividad profesional mientras pertenezcan a la plantilla de empleados de la UNED.

Cuando un usuario causa baja en la UNED, se aplicará lo siguiente:

1. Si la UNED lo considera necesario, el usuario deberá permitir el acceso a la información que hubiera en su ordenador de trabajo.
2. Para poder acceder a dicha información el trabajador facilitará su usuario y password al Responsable de la Unidad administrativa de la UNED, según el formulario recogido en el ANEXO I; a tal efecto, se cumplimentarán y se entregarán firmadas 2 copias, una para el usuario y otra para el Responsable de la Unidad.
3. Si el empleado no facilitara su usuario y password, la UNED autorizará al Técnico informático a desbloquear la seguridad del sistema, con el fin de que el Responsable del Servicio pueda acceder a la información y a los datos contenidos en el ordenador según el ANEXO II; a tal efecto, se cumplimentarán y se entregarán firmadas 2 copias, una para el Técnico Informático y otra para el Responsable del Servicio de la UNED.

## ANEXO I

### Autorización de acceso a la información y a los datos en un ordenador de un puesto de trabajo

D/D<sup>a</sup>: \_\_\_\_\_

Autorizo al Responsable de mi Unidad administrativa a acceder a la información contenida en el ordenador de mi puesto de trabajo, por lo cual le facilito mi usuario y mi password:

USUARIO: \_\_\_\_\_

PASSWORD: \_\_\_\_\_

Fecha: \_\_\_\_\_

Firma del usuario:

Firma del Responsable de la Unidad administrativa:

## ANEXO II

### Autorización de acceso al Técnico Informático al ordenador del usuario

D/D<sup>a</sup>: \_\_\_\_\_, como  
Responsable del Servicio de la UNED autorizo al Técnico Informático D/D<sup>a</sup>: \_\_\_\_\_  
\_\_\_\_\_ a acceder al ordenador del puesto de trabajo  
del usuario D/D<sup>a</sup>: \_\_\_\_\_ para facilitar al  
Responsable del Servicio la información y los datos que sean de su interés.

Fecha: \_\_\_\_\_

Firma del Responsable del Servicio:

Firma del Técnico Informático:



## **ANEXO 4.6.**

# **PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS EN LOS FICHEROS AUTOMATIZADOS CON DATOS DE CARÁCTER PERSONAL DE LA UNED**

**Departamento de Política Jurídica de Seguridad  
de la Información de la UNED**

## ÍNDICE

1. OBJETO.....	3
2. ¿QUÉ ES UNA INCIDENCIA? .....	3
3. PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENCIAS DE FICHEROS AUTOMATIZADOS .....	3

## 1. OBJETO

Establecer el procedimiento para que todas las incidencias recibidas en el Centro de Atención al Usuario (CAU) relativas a la pérdida o recuperación de datos de carácter personal, se comuniquen a la Sección de Protección de Datos y puedan ser registradas en el Documento de Seguridad, cumpliendo así con lo legalmente establecido.

## 2. ¿QUÉ ES UNA INCIDENCIA?

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

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

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

- La pérdida de contraseñas de acceso a los Sistemas de Información
- El uso indebido de contraseñas (su divulgación, la utilización de contraseñas de otros usuarios, no cambiarla en periodos superiores a un año, etc.)
- El acceso no autorizado a ficheros, sin el perfil correspondiente
- La pérdida de soportes informáticos con datos de carácter personal
- La pérdida de datos por el mal uso de las aplicaciones
- Infección de los sistemas de información por virus u otros elementos dañinos

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

## 3. PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENCIAS RELATIVAS A FICHEROS AUTOMATIZADOS

1. Una vez producida la incidencia, el usuario conocedor de la misma, debe comunicarla al Centro de Atención al Usuario (CAU) telefónicamente o a través de las direcciones: [soportePAS@csi.uned.es](mailto:soportePAS@csi.uned.es) o [soportePDI@csi.uned.es](mailto:soportePDI@csi.uned.es)
2. Informará al Responsable del fichero o en su defecto al Responsable directo de su Unidad.

3. En el caso de que se hayan visto afectados ficheros con datos de nivel medio o alto y sea necesario llevar a cabo algún procedimiento de recuperación de datos, será imprescindible que el Responsable del Fichero autorice la ejecución del citado procedimiento. Para ello el CAU deberá requerir al usuario la citada autorización.
4. El personal del CAU tomará las medidas oportunas para que, en el menor tiempo posible, se subsane la anomalía que haya generado la incidencia.
5. El CAU remitirá, mensualmente, al Departamento de Política Jurídica de Seguridad de la Información un informe en formato Excel, con las incidencias producidas y que afecten a los datos de carácter personal, a la dirección del correo electrónico [dptojuridicoseguridad@adm.uned.es](mailto:dptojuridicoseguridad@adm.uned.es) para su registro en el Documento de Seguridad.



## **ANEXO 4.7.**

# **PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS EN LOS FICHEROS NO AUTOMATIZADOS O PAPEL CON DATOS DE CARÁCTER PERSONAL DE LA UNED**

## ÍNDICE

<b>1. OBJETO</b> .....	<b>3</b>
<b>2. ¿QUÉ ES UNA INCIDENCIA?</b> .....	<b>3</b>
<b>3. PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENCIAS RELATIVAS A FICHEROS NO AUTOMATIZADOS O PAPEL</b> .....	<b>3</b>

## 1. OBJETO

Establecer el procedimiento para que todas las incidencias producidas y relativas a la pérdida o recuperación de datos de carácter personal, en formato papel, se comuniquen al Departamento de Política Jurídica de Seguridad de la Información, para que puedan ser registradas en el Documento de Seguridad, cumpliendo así con lo legalmente establecido.

## 2. ¿QUÉ ES UNA INCIDENCIA?

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

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

Ejemplos de incidencias comunes que pudieran afectar a los datos personales contenidos en ficheros no automatizados o en papel son los siguientes:

- La pérdida de las llaves de acceso a los archivos, armarios y dependencias, donde se almacena la información de carácter personal
- El uso indebido de las llaves de acceso
- El acceso no autorizado de usuarios a los archivos, armarios y dependencias, donde se encuentran ficheros con datos de carácter personal
- La pérdida de soportes o documentos en papel con datos de carácter personal
- El deterioro de los soportes o documentos, armarios y archivos, donde se encuentran datos de carácter personal

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

## 3. PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENCIAS RELATIVAS A FICHEROS NO AUTOMATIZADOS O PAPEL

1. Una vez producida la incidencia el usuario, conocedor de la misma, debe cumplimentar el formulario correspondiente que se encuentra en el Portal Web UNED, espacio PROTECCIÓN DE DATOS (con autenticación).

a) **Modelo de notificación de incidencias de ficheros de nivel básico en papel**

b) **Modelo de notificación de incidencias de ficheros de nivel medio y alto en papel**

2. Informará al Responsable del fichero o en su defecto al Responsable directo de su Unidad.
3. A continuación le usuario, remitirá el formulario al Departamento de Política Jurídica de Seguridad de la Información a través de la dirección: [incidenciaslopd@adm.uned.es](mailto:incidenciaslopd@adm.uned.es)
4. El personal del Departamento registrará la incidencia en el Documento de seguridad y velará para que se tomen las medidas oportunas y que, en el menor tiempo posible, se subsane la anomalía que haya generado la incidencia.

**NOTIFICACIÓN DE INCIDENCIAS QUE AFECTEN A DATOS DE CARÁCTER PERSONAL DE NIVEL BÁSICO, EN PAPEL**

<b>FECHA DE LA NOTIFICACIÓN</b>	Haga clic aquí para escribir una fecha.
<b>FECHA Y HORA DE LA INCIDENCIA</b>	Haga clic aquí para escribir una fecha. HORA:
<b>DESCRIPCIÓN DE LA INCIDENCIA</b>	
<b>PERSONA QUE NOTIFICA</b>	<b>NOMBRE Y APELLIDOS:</b> <b>UNIDAD:</b> <b>PUESTO:</b>
<b>PERSONA A QUIEN SE COMUNICA LA INCIDENCIA</b> <b>RESPONSABLE DEL FICHERO (en su caso)</b> <b>FICHERO AFECTADO (en su caso)</b>	<b>NOMBRE Y APELLIDOS:</b> <b>PUESTO:</b> Elija un elemento. Elija un elemento.

**NOTIFICACIÓN DE INCIDENCIAS QUE AFECTEN A DATOS DE CARÁCTER PERSONAL DE NIVEL MEDIO /ALTO  
EN PAPEL**

<b>FECHA DE LA NOTIFICACIÓN</b>	Haga clic aquí para escribir una fecha.
<b>FECHA Y HORA DE LA INCIDENCIA</b>	Haga clic aquí para escribir una fecha. <b>HORA:</b>
<b>DESCRIPCIÓN DE LA INCIDENCIA</b>	
<b>PERSONA QUE NOTIFICA</b>	<b>NOMBRE Y APELLIDOS:</b> <b>UNIDAD:</b> <b>PUESTO:</b>
<b>PERSONA A QUIEN SE COMUNICA LA INCIDENCIA</b>	<b>NOMBRE Y APELLIDOS:</b> <b>PUESTO:</b>
<b>RESPONSABLE DEL FICHERO (en su caso)</b>	Elija un elemento.
<b>FICHERO AFECTADO (en su caso)</b>	Elija un elemento.
<b>NIVEL DE SEGURIDAD</b>	Elija un elemento.
<b>EFFECTOS QUE PUEDE PRODUCIR LA INCIDENCIA</b>	
<b>MEDIDAS CORRECTORAS APLICADAS</b>	



## **ANEXO 4.8.**

# **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNED**

**(Aprobada por el Consejo de Gobierno el 13 de diciembre de 2016)**

## INTRODUCCIÓN

La Universidad Nacional de Educación a Distancia (UNED) es una institución de derecho público, dotada de personalidad jurídica y de plena autonomía en el desarrollo de sus funciones, sin más limitaciones que las establecidas en las leyes.

Desde su creación, la implantación de las Tecnologías de la Información y de las Comunicaciones (TIC) ha supuesto un gran avance en la calidad del servicio público de la educación superior que se presta.

El documento fundamental para abordar la normativa de seguridad de la UNED, es su Política de Seguridad de la Información, que establece los principios y directrices a tener en cuenta en su posterior desarrollo normativo y define la estructura organizativa de la seguridad de la información.

La Política de Seguridad de la Información se elabora en cumplimiento de la exigencia del **Real Decreto 3/2010**, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad (ENS)** en el ámbito de la Administración Electrónica, que en su artículo 11 establece la obligación de las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir, que será aprobada por el titular del órgano superior correspondiente.

En el Preámbulo indica que los sistemas de información de las Administraciones pretenden:

*“La creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes.*

*De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y **los responsables de cada dominio de seguridad deben coordinarse efectivamente** para evitar “tierras de nadie” y fracturas que pudieran dañar a la información o a los servicios prestados”.*

El artículo 5 del ENS, “La seguridad como un proceso integral”, señala lo siguiente:

1. **La seguridad** se entenderá como un **proceso integral** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Su aplicación estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.
2. Se prestará la máxima atención a la **concienciación de las personas** que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

En el artículo 12 “Organización e implantación del proceso de seguridad” se determina que:

**La seguridad deberá comprometer a todos los miembros de la organización.** La política de seguridad según se detalla en el anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y **ser conocida por todos los miembros** de la organización administrativa.

En consecuencia, el presente documento fija los criterios básicos sobre el sistema de información de la UNED y, en concreto, las normas de uso del ordenador asignado al puesto de trabajo, la red corporativa, los equipos portátiles, las aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, tanto en soporte informático como en papel.

Asimismo, **La ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas** señala en su artículo 13, apartados a y b, los siguientes derechos de las personas:

*A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración y a ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.*

Por otro lado, la **ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público** preceptúa en su artículo 3 apartado 2 que:

*“Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados”.*

En virtud de lo expuesto, de conformidad con lo establecido, es compromiso de todos los miembros de la comunidad universitaria contribuir, desde sus respectivas responsabilidades, a la mejor realización del servicio público.

#### Aprobación de la Política de Seguridad de la Información de la UNED

El propósito de la presente Política de Seguridad de la Información de la UNED, es establecer las bases de la fiabilidad con que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas. En este documento se recoge el conjunto de medidas necesarias, tanto técnicas como organizativas, encaminadas a conseguir un nivel de protección adecuado con el fin de asegurar el cumplimiento legal, garantizar la disponibilidad y la confidencialidad de la información.

## ÍNDICE

- I. Política de Seguridad de la Información
- II. Misión y marco normativo de la UNED
- III. Principios de la seguridad de la información
- IV. Estructura Normativa
- V. Organización de la Seguridad
- VI. Protección de datos de carácter personal
- VII. Gestión de riesgos
- VIII. Formación y concienciación
- IX. Actualización y revisión periódica
- X. Entrada en vigor

### I.- Política de Seguridad de la Información

1.- La Política de Seguridad de la Información identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

2.-La consolidación del uso de las nuevas tecnologías en la UNED, exige el establecimiento de un conjunto de actividades y procedimientos para el tratamiento y gestión de los riesgos asociados a la seguridad de la información. La gestión de la seguridad de los sistemas de información es un proceso complejo que incluye a personas, tecnologías, normas y procedimientos.

3.-La Administración Electrónica permite que cualquier ciudadano o los miembros de la comunidad universitaria puedan realizar sus trámites desde cualquier lugar y en cualquier momento, a través del uso de técnicas y medios electrónicos, informáticos y telemáticos. De esta forma la iniciación, tramitación y terminación de los procedimientos puede

realizarse, con plena validez, en plenas condiciones de seguridad, y con interoperabilidad con otras Administraciones y conforme al Esquema Nacional de Seguridad y al Esquema Nacional de Interoperabilidad, Real Decreto 3/2010 y Real Decreto 4/2010 respectivamente.

4.-La Política de Seguridad de la Información pretende dar soporte al desarrollo, coordinación y racionalización de la normativa específica y a la actualización de los conceptos según la evolución de las TIC y de la legislación vinculante y alcanzar de esta forma un conjunto normativo equilibrado y completo.

## II.-Misión y Marco Normativo de la UNED

El art. 3.1 de Los Estatutos de la UNED, (R.D. 1239/2011, de 8 de septiembre por el que se aprueban los Estatutos de la Universidad Nacional de Educación a Distancia) establece como fines de la UNED, el desempeño del servicio público de la educación superior mediante la investigación, la docencia y el estudio.

La UNED reconoce como funciones esenciales de su actividad la enseñanza, el estudio, la investigación y la transferencia del conocimiento, en orden al pleno desarrollo científico, cultural, artístico y técnico de la sociedad (art.7 Estatutos).

La misión de la UNED es la de “desempeñar el servicio público de la educación superior mediante la docencia, el estudio, la investigación y la transferencia del conocimiento, asumiendo el compromiso de facilitar al máximo el acceso a la enseñanza universitaria, la continuidad de estudios y la formación a lo largo de la vida a todo tipo de personas. Todo ello mediante la aplicación de una metodología didáctica específica “a distancia” que combina las tecnologías más avanzadas con la tutorización personalizada presencial y digital”.

La derogada Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, marcó un hito significativo a la contribución de la implementación de la Administración Electrónica. Junto a este marco jurídico, podemos indicar en la tabla siguiente, otra normativa en relación a esta materia.

NORMATIVA GENERAL	OBJETIVO
Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas	Derecho de los ciudadanos a relacionarse mediante medios electrónicos con las Administraciones Públicas
Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público	Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos, que aseguren la seguridad
Real Decreto 3/2010, Esquema Nacional de Seguridad	Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información
Real Decreto 4/2010, Esquema Nacional de Interoperabilidad	Comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección Tecnológica

Ley 59/2003, de 19 de diciembre, de firma electrónica	Regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación
Real Decreto 1553/2005, de 23 de diciembre de 2005	Regula la expedición del documento nacional de identidad y sus certificados de firma electrónica
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal	Garantiza y protege, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar
Real Decreto 1720/2007, de 21 de diciembre	Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
Decreto 2310/1972, de 18 de agosto	Creación de la UNED
R.D. 1239/2011 de 8 septiembre	Estatutos de la UNED
Cualquier otra normativa que pueda aprobarse y resulte aplicable	

### III.- Principios de la seguridad de la Información

La presente Política de Seguridad de la información se basa en unos principios básicos de protección que forman los pilares sobre los que se sustentan y sustentarán todas las actuaciones en materia de seguridad que realice la Universidad. Se establecen los siguientes:

#### 1.- Principios Básicos:

- a) Alcance y concienciación: Todo el personal de la Universidad debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad.
- b) Responsabilidad diferenciada: En los sistemas de información se diferenciarán de forma clara el responsable de la información, el responsable del servicio y el responsable de seguridad.  
El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.  
La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.
- c) La seguridad como proceso integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando cualquier actuación que ponga en peligro este proceso.
- d) Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá estar permanentemente actualizado. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad.
- e) Profesionalidad: La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido, en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

- f) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto.

## 2.- Principios de protección de la seguridad de la información

La presente Política de Seguridad de la Información se basa en unos principios de protección que serán las bases de las actuaciones en materia de seguridad. Se establecen para ello las siguientes directrices:

- a) Protección de datos de carácter personal: La UNED, adoptará las medidas oportunas para garantizar el nivel de seguridad requerido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.
- b) Clasificación y control de activos: Los recursos informáticos y la información de la UNED, se encontrarán inventariados, con un responsable asociado. Los inventarios se mantendrán actualizados para asegurar su validez.
- c) Seguridad física y ambiental: Los sistemas de información serán emplazados en áreas seguras protegidas con controles de acceso físicos adecuados a la consideración de servicios críticos de los mismos. Los sistemas y los activos de información que contienen estarán suficientemente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.
- d) Gestión de la seguridad en comunicaciones y operaciones: La UNED, buscará los procedimientos necesarios para asegurar la correcta gestión, operación y actualización de las TIC, realizando una adecuada protección de la información, mediante mecanismos que garanticen su seguridad.
- e) Control de acceso: La UNED, mediante la implantación de mecanismos de identificación, autenticación y autorización facilitará y controlará el acceso a los sistemas de información de la Universidad. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y la comprobación del uso correcto.
- f) Desarrollo y mantenimiento de los sistemas de información: Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto, debiendo contemplarse los aspectos de seguridad en todas las fases del ciclo de vida de los sistemas de información.
- g) Gestión de la continuidad: La UNED, establecerá un sistema de detección y reacción ante incidentes de seguridad que se produzcan y las acciones de tratamiento a seguir,

para mantener la continuidad de los procesos y servicios, de acuerdo a las necesidades de los usuarios.

- h) Cumplimiento: La UNED, adoptará las medidas técnicas y organizativas necesarias para mantener sus sistemas de información adaptados a la normativa legal vigente, y en especial a las regulaciones legales relativas al tratamiento de datos de carácter personal, cuyas medidas específicas de tratamiento figuren en el correspondiente documento de seguridad.

#### IV.- Estructura Normativa

Debido a las competencias y funciones de la UNED, los temas que afectan a la seguridad de la información y su constante actualización, resulta imprescindible la estructuración de la normativa de seguridad de la información en distintos niveles relacionados de forma jerárquica:

1. Política de Seguridad
2. Normas de Seguridad
3. Procedimientos de Seguridad

El personal de la UNED, tendrá la obligación de conocer y cumplir las Normas y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones, así como la Política de Seguridad de la Información.

##### 1. Política de Seguridad de la Información

Constituye el primer nivel normativo. Se recoge en el presente documento y es aprobada por el Consejo de Gobierno, a propuesta del Comité de Seguridad de la Información.

##### 2. Normas de Seguridad de la Información

1. La Política de Seguridad de la Información se desarrollará por medio de la normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

2. Las Normas de Seguridad de la Información tienen aplicabilidad en toda la UNED, siendo el Consejo de Gobierno, el órgano responsable de la aprobación de las Normas.

### 3. Procedimientos de Seguridad de la Información

Los Procedimientos de Seguridad de la Información, están constituidos por instrucciones de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios. Serán aprobados por el Comité de Seguridad de la Información de la UNED.

## V. Organización de la Seguridad

Todos y cada uno de los usuarios de los sistemas de información de la UNED, son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

**Los cargos y puestos de trabajo que intervienen en la seguridad de la información de la UNED son los siguientes:**

Gerente de la UNED	Responsable de la Información
Vicerrector de Medios y Tecnología	Responsable de Seguridad de la Información
Vicegerente de RR.HH. y organización	Responsable del Servicio

Subdirector de los servicios al usuario	Responsable del Sistema
Coordinador de Sistemas de Tecnología de la Información (CIO)	
Secretaria General	
Jefa del Dpto. de Política Jurídica de Seguridad de la Información	
Administrador de la Seguridad del Sistema	
Asesor de Seguridad	
Jefa de la Sección de Protección de Datos	

La resolución rectoral con el nombramiento de los miembros del Comité de Seguridad de la Información de la UNED, figura en el ANEXO I.

#### VI. Protección de datos de carácter personal

La legislación sobre protección de datos de carácter personal establece una serie de responsables con funciones específicas.

- a) Los **Responsables de Ficheros de la UNED** son los órganos que para cada fichero se concreta en las Resoluciones de creación del mismo. Deciden sobre la finalidad, contenido y uso del tratamiento.
- b) Los **Responsables de Seguridad de la UNED** son el Coordinador de Sistemas de Tecnología de la Información (CIO), para los ficheros automatizados, y la Jefa de la Sección de Protección de Datos para los documentos en papel.
- c) La **Delegada de Protección de Datos de la UNED** es la Jefa del Departamento de Política Jurídica de Seguridad de la Información que debe asesorar y supervisar al responsable o al encargado del tratamiento en el cumplimiento de la normativa de protección de datos.
- d) El **documento de seguridad** relacionado con el tratamiento de datos de carácter personal debe ser aprobado, por el Comité de Seguridad.

## VII. Gestión de riesgos

- 1.- Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos, de manera continua sobre el sistema de información.
- 2.- Se repetirá de forma regular, al menos una vez cada dos años, cuando cambie la información manejada, los servicios prestados, cuando se detecte un incidente grave de seguridad o vulnerabilidades graves.
- 3.- El Comité de Seguridad propondrá la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.
- 4.- Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y de manera fundamental las guías del Centro Criptológico Nacional.

## VIII. Formación y concienciación

La UNED desarrollará, en ejercicio de la Disposición adicional primera del ENS, actividades formativas con la finalidad de concienciar a su personal en materia de seguridad de la información, difundiendo entre los usuarios la Política de Seguridad de la Información y su desarrollo normativo.

## IX.- Actualización y revisión periódica

La Política de Seguridad de la Información ha de mantenerse actualizada de forma permanente con la finalidad de adecuarla al progreso de los servicios de la Administración Electrónica, evolución de las nuevas tecnologías y de los sistemas de información.

La nueva legislación aprobada que sea aplicable así como, las normas derogadas serán actualizadas en la Política de Seguridad de la UNED, por el Comité. De igual forma se procederá a actualizar el nombramiento de los miembros del Comité que se renueven por Resolución Rectoral.

## X.- Entrada en vigor

La Política de Seguridad de la Información de la UNED, que se aprueba en esta Resolución, entrará en vigor a partir del día siguiente de su publicación en el BICI.

## ANEXO I Miembros del Comité de Seguridad de la Información de la UNED

### Rectorado

Este Rectorado, en uso de las atribuciones conferidas por el artículo 99 v) de los Estatutos de la Universidad y los artículos 10 y 29 del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, ha resuelto nombrar a los miembros del Comité de Seguridad de la Información de la UNED y la función a desempeñar en el mismo.

Agustín Torres Herrero	Responsable de la Información	Presidente del Comité
Juan Manuel Cigarrán Recuero	Responsable de la Seguridad de la Información	Vocal
Nicolás García Zorita	Responsable del Servicio	Vocal
José Calvo Calvo	Responsable del Sistema	Vocal
Antonio Sandoval Bonache	Coordinador de Sistemas de Tecnología de la Información (CIO)	Vocal
Almudena Rodríguez Moya	Secretaria General o persona en quien delegue	Vocal
Paz San Segundo Manuel	Jefa de Departamento de Política Jurídica de Seguridad de la Información	Vocal
Antonio Ruipérez García	Administrador de la Seguridad del Sistema	Vocal
Francisco Javier Martínez Martínez	Asesor de Seguridad	Asesor (con voz y sin voto)
Rosa Maján Martínez	Jefa de Sección de Protección de Datos	Secretaria del Comité (con voz y sin voto)

Sin perjuicio de la asistencia de los miembros antes citados, podrán asistir otros cargos o técnicos de la Universidad al Comité de Seguridad de la Información, cuando se trate de temas relacionados con el Esquema Nacional de Seguridad.

Madrid, 18 de diciembre 2017

EL RECTOR,



Firmado digitalmente por:  
Alejandro Tiana Ferrer  
Rector  
Tfno: 91 3986512  
rector@adm.uned.es

Alejandro Tiana Ferrer

ANEXO 4.9.1

## Secretaría General

- REGLAMENTO DEL SERVICIO DE INSPECCIÓN DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

(aprobado por el Consejo de Gobierno de 7 de marzo de 2011)

## REGLAMENTO DEL SERVICIO DE INSPECCIÓN DE LA UNED

Desde la aprobación del Reglamento de Funcionamiento de Régimen Interno del Servicio de Inspección, por la Junta de Gobierno, con fecha 17 de octubre de 1997, se han sucedido una serie de cambios legislativos que afectan al ámbito universitario y hacen aconsejable abordar una revisión del mismo.

En efecto, el punto de partida inicial que supuso el artículo 16.1 del Real Decreto 898/1985, de 30 de abril sobre Régimen de Profesorado Universitario con la previsión de creación de un Servicio de Inspección al que se le debían encomendar las tareas de inspeccionar el funcionamiento de sus servicios, y el seguimiento y control general de la disciplina académica, ha quedado superado por la posterior promulgación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, modificada a su vez, por la Ley 4/2007, de 12 de abril, cuya vocación es el diseño de la nueva arquitectura normativa que era reclamada por el sistema universitario español para mejorar su calidad docente, investigadora y de gestión, y su adecuación al nuevo Espacio Europeo de Educación Superior, siendo necesario para ello, según reza su Exposición de Motivos, que las Universidades incrementen de forma urgente su eficacia, eficiencia y responsabilidad, principios todos ellos centrales de la propia autonomía universitaria.

Asimismo, la Ley 7/2007, de 12 de abril que aprueba el Estatuto Básico del Empleado Público aspira a ordenar el sistema de empleo público en su conjunto, incluyendo una regulación general de los deberes de los empleados públicos, fundada en principios éticos y reglas de comportamiento que constituye un auténtico código de conducta, además de someter el régimen disciplinario de funcionarios públicos y personal laboral a sus previsiones.

Por último, el Real Decreto 1791/2010, de 30 de diciembre, por el que se aprueba el Estatuto del Estudiante Universitario realiza una serie de previsiones relacionadas con el régimen disciplinario de este sector de la comunidad universitaria que deben ser tenidas en consideración.

La UNED ha seguido esta línea marcada por la legislación en la última modificación de sus Estatutos, en los que ha incluido el Servicio de Inspección, con objeto de contribuir al mejor funcionamiento de todos

sus servicios y asumir la instrucción de todos los expedientes disciplinarios, junto al seguimiento y control general de la disciplina académica.

Estos objetivos responden al firme compromiso adquirido por nuestra Universidad para la mejora continua en sus ámbitos de actuación: docencia, investigación y prestación de servicios universitarios. Todo ello promoviendo un modelo de funcionamiento coordinado, transparente, eficiente y orientado a dar respuesta a las necesidades de los diferentes colectivos universitarios.

El presente Reglamento responde tanto a la necesidad

de cumplir con el mandato estatutario, como a la de dotar al Servicio de Inspección de un contenido funcional y flexible que le permita adaptarse a la realidad universitaria, centrando sus esfuerzos no sólo en el control del cumplimiento de la normativa y de los procesos internos de los distintos órganos y unidades, sino también en garantizar una mejora en la calidad de la prestación de los servicios, gestionados desde una mayor eficiencia de los recursos disponibles.

En su virtud, se aprueba el siguiente,

### REGLAMENTO DEL SERVICIO DE INSPECCIÓN DE LA UNED

#### Capítulo I: De la competencia y ámbito de actuación del Servicio de Inspección

##### Art. 1º.- Naturaleza Jurídica y Misión.

El Servicio de Inspección es una unidad de atención a la comunidad universitaria que se configura con un triple objetivo:

- a) técnico, para comprobar el cumplimiento de los acuerdos del Consejo de Gobierno;
- b) consultivo, para informar y asesorar a las diferentes instancias de gobierno de la UNED, a fin de contribuir al mejor funcionamiento de todos los servicios;
- c) y disciplinario, para asumir la instrucción de todos los expedientes disciplinarios a que haya lugar, garantizando, asimismo, el seguimiento y control general de la disciplina académica.

##### Art. 2º.- Ámbito de aplicación.

**2.1.** El Servicio de Inspección ejercerá sus funciones de índole técnica, respecto de las Facultades, Escuelas y demás Centros docentes adscritos a la Universidad, y cualesquiera Departamentos, Servicios y Unidades administrativas pertenecientes a la misma.

**2.2.** Asimismo, ejercerá sus funciones de índole disciplinaria sobre el personal docente e investigador, personal de administración y servicios, y estudiantes que conforman la comunidad universitaria.

**2.3.** En relación con los profesores tutores ejercerá, en su caso, las competencias establecidas por la normativa correspondiente.

##### Art. 3º.- Funciones.

El Servicio de Inspección ejercerá las siguientes funciones, a instancia del Rector o, en su caso, de los órganos competentes, según el plan de actuación aprobado:

- a) Velar por el correcto funcionamiento y la calidad de los servicios de la Universidad.
- b) La inspección del funcionamiento de los servicios de la Universidad, tanto de los dedicados a la docencia e investigación, como a la administración y gestión, teniendo en cuenta el seguimiento de objetivos y con según los principios de legalidad, eficacia, eficiencia y calidad.

- c) La información y asesoramiento a los responsables de las Facultades, Escuelas, Departamentos y demás unidades de servicio a la docencia e investigación, así como a los responsables de los Servicios administrativos, en las materias que sean competencia del Servicio de Inspección, como apoyo al mejor desarrollo de las tareas que a aquéllos corresponden.
- d) Colaborar en el seguimiento y control general de la disciplina académica, sin perjuicio de las competencias asignadas a las Facultades, Escuelas y Departamentos, a fin de garantizar la debida atención a los estudiantes y de salvaguardar los derechos de todos los implicados.
- e) Colaborar con las estructuras académicas o administrativas de la UNED en la propuesta de incoación de expedientes disciplinarios, competencia ésta, exclusiva del Rector y, en su caso, la realización de las informaciones previas a dicha propuesta de incoación.
- f) La instrucción de todos los expedientes disciplinarios que se incoen a cualquiera de los miembros de la comunidad universitaria. A estos efectos, cuando se proceda al nombramiento de un Instructor o de un encargado de una información previa que no pertenezca al Servicio de Inspección, éste quedará adscrito temporalmente a dicho Servicio como colaborador.
- g) Elaborar la propuesta de resolución de los expedientes disciplinarios que será elevada al Rector para que, en su caso, dicte la resolución que corresponda.
- h) Recabar de las Facultades, Escuelas, Departamentos, Programas, Unidades y Servicios de la Universidad los informes que considere necesarios en orden al mejor cumplimiento de sus funciones.
- i) Informar al Rector puntualmente de los aspectos más relevantes de las actuaciones desarrolladas.
- j) Tramitar, a instancia del Rector o del Consejo Social, las solicitudes de realización de informes e inspección dirigidas a las Administraciones Públicas a que se refiere el Real Decreto 898/85, de 30 de abril.
- k) Presentar al Consejo de Gobierno, con carácter anual, un informe en el que se expresen las actividades y funcionamiento del Servicio, así como las sugerencias que el mismo ofrezca sobre su capacidad operativa para el mejor servicio a la Universidad.
- l) Informar a la Junta de Personal Docente, a la Junta de Personal de Administración y Servicios y al Comité de Empresa de la Universidad de las actuaciones de su competencia en el marco de la legislación aplicable, con respeto, en todo caso, al derecho a la intimidad y al deber de confidencialidad.
- m) Instruir, a propuesta del órgano competente, los expedientes de revocación de la "venia docendi" a los profesores tutores, en los supuestos previstos y según el procedimiento establecido por la normativa reguladora de la función tutorial. Así como elevar al Rector la correspondiente propuesta de resolución.
- n) Cualquier otra que le pueda ser encomendada por el

Rector, dentro del marco de las funciones recogidas en este Reglamento.

#### **Art. 4º.- Competencia para resolver los expedientes disciplinarios.**

La resolución de los expedientes disciplinarios y la aplicación de las sanciones pertinentes serán, en todo caso, competencia del Rector, salvo las de separación del servicio, de acuerdo con lo establecido en la legislación aplicable en materia disciplinaria del personal al servicio de las Administraciones Públicas.

## **Capítulo II. De la Estructura del Servicio de Inspección**

### **Art. 5º.- Dependencia y composición.**

**5.1.** El Servicio de Inspección, dependerá directamente del Rector y gozará de la necesaria autonomía funcional para poder desarrollar sus actuaciones en el ámbito de la Universidad.

**5.2.** Estará integrado por un Director, un Subdirector, en su caso, y hasta un máximo de doce vocales, que actuarán cuando las necesidades del servicio lo requieran. Asimismo, contará con una estructura administrativa idónea para el desarrollo de sus funciones.

**5.3.** La relación de puestos de trabajo del personal funcionario de administración y servicios de la UNED deberá contemplar la estructura que precise el Servicio de Inspección.

### **Art. 6º.- El Director del Servicio de Inspección.**

**6.1.** El Servicio de Inspección ejercerá sus funciones bajo la dirección inmediata de un Director que, con categoría de Vicerrector, será nombrado por el Rector entre los vocales, oído el Consejo de Gobierno.

**6.2.** La duración del mandato del Director del Servicio de Inspección será de cuatro años y podrá ser prorrogado por una sola vez consecutiva.

**6.3.** En el supuesto de recaer el nombramiento de Director en un miembro del personal docente, podrá ser dispensado parcialmente de su carga docente, o en caso de que fuera miembro del personal de administración y servicios, de los cometidos propios de su puesto de destino, cuando así lo exija el cumplimiento de sus funciones.

### **Art. 7º.- Funciones del Director del Servicio de Inspección.**

Serán funciones del Director del Servicio de Inspección:

- a) Ejercer la dirección y coordinar, con criterios de homogeneidad y eficacia, la actividad inspectora de los miembros adscritos al Servicio de Inspección.
- b) Elaborar, de acuerdo con los miembros del Servicio, el plan general de actuación inspectora que tendrá carácter anual.
- c) Establecer los criterios de organización interna para el mejor funcionamiento del Servicio.
- d) Proponer al Rector, cuando así proceda, el nombramiento de un Subdirector del Servicio.
- e) Proponer al Rector los vocales adscritos al Servicio

que deban actuar en cada una de las acciones inspectoras, como Instructor o Secretario, en su caso.

- f) Elevar los informes, propuestas o sugerencias del Servicio e informar periódicamente al Rector del desarrollo de la función inspectora en los distintos ámbitos funcionales del Servicio y emitir, en consecuencia, las propuestas de actuación que procedan.
- g) Participar, como miembro nato, en la Comisión de Responsabilidad Social de la UNED y en cualquier otro órgano consultivo o de participación cuando así lo establezca la regulación propia de la UNED.
- h) Realizar cuantas tareas inspectoras de carácter urgente o puntual le encomiende el Rector.

#### **Art. 8º.- El Subdirector del Servicio de Inspección.**

El Director del Servicio de Inspección podrá, en su caso, proponer al Rector el nombramiento de un Subdirector de entre los vocales del Servicio, al que le serán encomendadas las funciones que determine el Director, a quien sustituirá en caso de ausencia, vacante o enfermedad.

#### **Art. 9º.- Los vocales del Servicio de Inspección.**

**9.1.** Los vocales del Servicio de Inspección serán nombrados y cesados por el Rector, oído el Consejo de Gobierno, de entre los miembros pertenecientes al Personal Docente e Investigador y Personal de Administración y Servicios que tengan la condición de funcionario público, por un período de dos años, que podrá ser renovado. Llevarán a cabo sus funciones bajo la dependencia jerárquica del Director del Servicio de Inspección.

**9.2.** En el supuesto de recaer el nombramiento de vocal en personal docente, podrá ser dispensado parcialmente de su carga docente, o en caso de que fuera miembro del personal de administración y servicios, de los cometidos propios de su puesto de destino, cuando así lo exija el cumplimiento de sus funciones.

#### **Art. 10º.- Indemnizaciones por razones del Servicio.**

El personal adscrito al Servicio de Inspección tendrá derecho a la percepción de las indemnizaciones que por razón de servicio les correspondan.

### **Capítulo III. Funcionamiento**

#### **Art. 11º.- Ejercicio de funciones consultivas.**

**11.1.** El Servicio de Inspección, como órgano consultivo, emitirá informes o recomendaciones a petición del Rector.

**11.2.** El Claustro, el Consejo de Gobierno o sus Comisiones Delegadas, el Consejo Social y los Órganos Colegiados establecidos en los Estatutos de la Universidad podrán solicitar dichos informes a través del Rector.

**11.3.** Cualquier miembro de la comunidad universitaria, mediante escrito dirigido al Rector, podrá poner en conocimiento de éste aquellos hechos que considere que pudieran ser competencia del citado Servicio.

#### **Art. 12º.- Funciones de Inspección de servicios.**

El Servicio de Inspección emitirá, de oficio o a instancia del Rector, notas informativas para el Claustro y el Consejo de Gobierno sobre el grado de cumplimiento y nivel de adecuación de los acuerdos tomados por estos órganos superiores de gobierno.

#### **Art. 13º.- Informes y recomendaciones.**

**13.1.** Los informes y recomendaciones emitidos por el Servicio de Inspección tendrán carácter técnico y se incorporarán a los expedientes de reforma, modificación o implantación de cualquier estructura, organismo o asunto para el que hayan sido requeridos.

**13.2.** Los informes y recomendaciones del Servicio de Inspección, emitidos a petición de los órganos de gobierno mencionados en el artículo decimoprimer de este Reglamento, tendrán también carácter público y deberán ser incorporados a la Memoria anual de la Universidad.

#### **Art. 14º.- Atribuciones del Servicio de Inspección.**

En el ejercicio de sus funciones, el Servicio de Inspección tendrá las atribuciones siguientes:

- a) Visitar, previo conocimiento de la autoridad competente, a efectos de obtener información directa y precisa, las Facultades, Escuelas, Departamentos, Unidades de Administración y de Servicios o Centros Asociados en los que se desarrollen actividades promovidas o autorizadas por la Universidad. En estas visitas los funcionarios del Servicio de Inspección recibirán de los miembros de la comunidad universitaria la ayuda y colaboración necesarias para el desarrollo de su actividad. Los responsables de las unidades inspeccionadas habilitarán los espacios adecuados, y los medios necesarios para facilitar las labores del Servicio de Inspección. En caso de incumplimiento de los deberes de información, ayuda y cooperación, el Servicio pondrá el hecho en conocimiento del Rector a los efectos que procedan.
- b) Realizar, en su caso, citaciones de comparecencia personal a los posibles implicados en, informaciones previas o reservadas, expedientes de revocación de "venia docendi" y procedimientos disciplinarios a fin de obtener de los mismos las informaciones oportunas, la rectificación o ratificación de datos o hechos, en aplicación de la normativa sobre procedimiento administrativo, incluso antes de adoptar decisiones sobre incoación de expedientes disciplinarios. Los requeridos podrán ser acompañados por un asesor de su libre designación.

#### **Art. 15º.- Acreditación del personal adscrito al Servicio de Inspección.**

El personal adscrito al Servicio de Inspección, para un correcto desempeño de sus tareas, estará identificado mediante una acreditación expedida por la Universidad, que deberá exhibir en cuantas actuaciones le sea requerida.

**Art. 16°.- Garantías del personal adscrito al Servicio de Inspección.**

El Director, el Subdirector y los vocales del Servicio de Inspección, en el ejercicio de sus funciones, gozarán de independencia, respecto de las autoridades de las que dependan los servicios y el personal objeto de inspección; y de inmunidad, no pudiendo ser sancionado o expedientado el personal adscrito al mismo, por opiniones, recomendaciones, sugerencias o informes que realicen con motivo de su actuación inspectora.

**Art. 17°.- Medios materiales de apoyo.**

El Servicio de Inspección, para el adecuado desarrollo de sus funciones, recabará de la Gerencia el apoyo jurídico, administrativo y técnico que considere necesario.

**Art. 18°.- Confidencialidad.**

Las actuaciones realizadas por el Servicio de Inspección en el ejercicio de sus funciones, incluyendo la documentación obrante en los expedientes, informes o propues-

tas, tendrán carácter confidencial. Asimismo, el personal integrante del Servicio de Inspección o que resulte temporalmente adscrito al mismo, estarán obligados al deber de sigilo o secreto por razón de su cargo o función.

**DISPOSICION DEROGATORIA**

Queda derogado el anterior Reglamento de Funcionamiento Interno del Servicio de Inspección de la UNED, aprobado por la Junta de Gobierno el 17 de octubre de 1997 (BICI de 9 de febrero de 1998).

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en el presente Reglamento.

**DISPOSICION FINAL**

El presente Reglamento entrará en vigor al día siguiente de su publicación en el Boletín Interno de Coordinación Informativa (BICI).

## **Modificación del Reglamento del Servicio de Inspección aprobado en Consejo de Gobierno (14.10.2014 y BICI de 03.11.14)**

### **a) Naturaleza jurídica y misión**

**(art.1)** Incluir en el apartado c):

c) mediador y disciplinario, para someter al ámbito de la mediación aquellos conflictos en que así se considere; y para asumir la instrucción de todos los expedientes disciplinarios a que haya lugar, garantizando, asimismo, el seguimiento y control de la disciplina académica.

### **b) Ámbito de aplicación (art. 2)**

Deberá incluirse en el apartado 2.2:

2.2 Asimismo, ejercerá sus funciones de índole mediadora y disciplinaria sobre el personal docente e investigador, personal de administración y servicios, y estudiantes que conforman la comunidad universitaria.

### **c) Funciones (art. 3)**

Deberá añadirse un nuevo apartado n), quedando el actual como apartado o):

n) Ofrecer la comunidad universitaria la posibilidad de someter a mediación aquellos conflictos susceptibles de solución acordada entre las partes.

### **d) Dependencia y composición del Servicio de Inspección (art.5)**

Deberá incluirse un nuevo apartado 5.3, quedando el actual punto 5.3 como punto 5.4.

*5.4.- El Servicio de Inspección contará dentro de su estructura con un Centro de Mediación.*

### **e) Funciones del Director del Servicio de Inspección (art.7)**

Añadir la expresión "mediadoras" a los párrafos f) y h) del art. 7:

f) Elevar los informes, propuestas o sugerencias del servicio e informar periódicamente al Rector del desarrollo de la función mediadora e inspectora en los distintos ámbitos funcionales del Servicio y emitir, en consecuencia, las propuestas de actuación que procedan.

g) Realizar cuantas tareas mediadoras e inspectoras de carácter urgente o puntual le encomiende el Rector.

## ANEXO 5.1.

### CLÁUSULA A INSERTAR EN UN CONTRATO, ACUERDO O CONVENIO EXISTENTE

#### **DEL ACCESO POR PARTE DEL PRESTADOR DE SERVICIOS A LOS DATOS DE CARÁCTER PERSONAL DE LOS FICHEROS TITULARIDAD DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED)**

Para la realización de los trabajos contratados, el *PRESTADOR DE SERVICIOS* tiene acceso a la información de carácter personal responsabilidad de la UNED. En cumplimiento de las obligaciones establecidas en el artículo 12 de la LOPD, las partes formalizan a través del presente documento, los términos en los que podrá realizarse dicho acceso:

1. La UNED autoriza, expresamente, a que el *PRESTADOR DE SERVICIOS* acceda a la información de carácter personal contenida en los ficheros titularidad del primero, con la única finalidad de llevar a cabo los servicios recogidos en este contrato y en el ANEXO I.
2. En el caso de que el *PRESTADOR DE SERVICIOS* someta a tratamiento o almacene, de cualquier modo, datos personales de los ficheros titularidad de la UNED, se compromete a adoptar las medidas de seguridad aplicables en función de la naturaleza de la información de carácter personal, según lo dispuesto en los artículos 89 a 114 del 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 (RLOPD). Así, deberá adoptar las medidas, técnicas y organizativas, que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico natural.
3. Asimismo, para el caso en que el servicio implique tratamiento de datos personales en las propias instalaciones del Encargado de Tratamiento, además de adoptar las medidas de seguridad correspondientes, elaborará un Documento de Seguridad o completará el que ya dispusiera, en su caso, identificando al Responsable de Fichero e incluyendo el/los fichero/s o tratamiento/s de datos personales que pertenece/n a éste, así como asociando las medidas de seguridad a implantar en relación con dicho tratamiento (art. 82.2. RLOPD).
4. El Responsable de Fichero o Tratamiento tendrá la facultad de exigir al Encargado de Tratamiento, prueba del cumplimiento de las obligaciones impuestas por la legislación de protección de datos, solicitando copia del Documento de Seguridad (al menos en la parte que le afecte), del informe de Auditoría, o de cualquier otro documento que estime conveniente siempre que se refiera a datos personales que trata por cuenta de aquél. En el supuesto de que no quede acreditada, a juicio del Responsable del Fichero

- o Tratamiento, el cumplimiento de las obligaciones que como Encargado de Tratamiento le corresponden, el primero podrá rescindir unilateralmente el contrato.
5. Las solicitudes de ejercicio de derechos de acceso, rectificación, cancelación y, en su caso, oposición, que puedan ser presentadas por parte de los interesados se ejercerán ante el Responsable del Fichero o Tratamiento. Si el Encargado de Tratamiento recibiese una petición de ejercicio de derechos deberá informar al interesado o afectado [titular de los datos] de la identidad del Responsable del Fichero, para que aquél se dirija al mismo.
  6. Queda terminantemente prohibida la aplicación o utilización de la información de carácter personal con un fin distinto al previsto en el presente contrato, así como su cesión o comunicación a terceros, ni siquiera para su conservación.
  7. En caso de que el PRESTADOR DE SERVICIOS utilizara los datos de carácter personal para finalidades distintas a las aquí señaladas, o los cediera o comunicara a terceros, incumpliendo las estipulaciones del presente contrato, será considerado, a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido y, especialmente, las derivadas del incumplimiento de lo dispuesto en la LOPD.
  8. El Responsable de Fichero autoriza al Encargado de Tratamiento para que subcontrate, en nombre y por cuenta del primero, el tratamiento de los datos necesarios para la prestación de los servicios objeto de subcontratación. Para ello, el Encargado de Tratamiento deberá informar previamente al Responsable de Fichero de la identidad de la persona física o jurídica a la cual pretende él subcontratar una parte o la totalidad de los servicios objeto de este contrato, así como la descripción de los servicios que serían objeto de esta subcontratación. La validez de la autorización ( que deberá constar por escrito) , quedará sujeta a la firma de un contrato escrito entre el Encargado de Tratamiento y el Subcontratista, que recoja términos análogos a los previstos en este contrato con el contenido íntegro establecido en el artículo 12 de la LOPD y a la asunción expresa por el Encargado de Tratamiento en su propio nombre y el Subcontratista de una responsabilidad solidaria por cualquier incumplimiento de los términos del tratamiento por este último.
  9. En todo caso, el Encargado de Tratamiento deberá entregar al Responsable del Fichero o Tratamiento una copia del contrato suscrito con la persona física o jurídica subcontratada, teniendo facultad el Responsable del Fichero de revocar el contrato y denegar la posibilidad de subcontratar, de no cumplir con la normativa vigente aplicable. En este caso, el Encargado de Tratamiento será el único responsable del destino de la información o documentación que hubiere comunicado al Subcontratista, debiendo en su caso ser recuperada y asegurándose que éste no almacena copia alguna.

10. Una vez finalizada la prestación contractual, los datos de carácter personal deben ser devueltos al Responsable del Fichero o Tratamiento, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de tratamiento, excepto cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el Responsable del Fichero o Tratamiento dicha conservación.
  
11. Aquellos datos que no se devuelvan deberán destruirse adoptando las medidas de seguridad para evitar el acceso por parte de terceros. También podrá el Encargado del Tratamiento conservar los datos de carácter personal, debidamente bloqueados, en tanto puedan derivarse responsabilidades de su relación con el Responsable del Fichero o Tratamiento.

En Representación de la UNED,

En Representación de.....,

## ANEXO I

### FINALIDADES QUE JUSTIFICAN EL ACCESO POR PARTE DEL ENCARGADO DE TRATAMIENTO

**1. INTRODUCCIÓN.-** El presente Anexo forma parte del contrato de acceso a datos suscrito entre las partes y detalla los ficheros a los que accede o trata el Encargado de Tratamiento, la tipología de datos, el nivel de seguridad a adoptar por el Encargado de Tratamiento y las finalidades que justifican el tratamiento

### 2. ACCESO POR PARTE DEL ENCARGADO DE TRATAMIENTO

#### NOMBRE DEL FICHERO AL QUE ACCEDE O TRATA EL ENCARGADO DE TRATAMIENTO

#### TIPOLOGÍA DE DATOS PERSONALES QUE CONTIENEN LOS FICHEROS:

**Datos de identificación** [Nombre y Apellidos, DNI, Nº SS, Dirección, Teléfono, Firma/Huella, Imagen/Voz]

**Datos especialmente protegidos** [Salud, Afiliación Sindical, Religión, Ideología, Creencias, Vida Sexual, Origen racial o étnico, Violencia de género]

**Datos de características personales** [Datos de estado civil; Edad; Datos de familia; Sexo; Fecha de nacimiento; Nacionalidad; Lugar de nacimiento; Idioma]

**Datos académicos y profesionales** [Formación; Titulaciones; Historial del estudiante; Experiencia profesional; Pertenencia a Colegios o Asociaciones profesionales]

**Datos detalle de empleo** [Cuerpo/Escala; Categoría/grado; Puestos de trabajo; Datos no económicos de nómina; Historial del trabajador]

**Datos económico-financieros y de seguros** [Ingresos, rentas; Inversiones, bienes patrimoniales; Créditos, préstamos, avales; Datos bancarios; Planes de pensiones, jubilación; Datos económicos de nómina; Datos deducciones impositivas/impuestas; Seguros; Hipotecas; Subsidios, beneficios; historial créditos; Tarjetas crédito]

**Datos de información comercial** [Actividades, Negocios; Suscripción a publicaciones]

**Datos de transacciones de bienes o servicios** [bienes o servicios suministrados por el interesado; bienes o servicios recibidos por el interesado]

**Otros:**

<b>NIVEL DE SEGURIDAD A ADOPTAR POR EL ENCARGADO DE TRATAMIENTO</b>	<b>BÁSICO</b>
	<b>MEDIO</b>
	<b>ALTO</b>

**FINALIDADES QUE JUSTIFICAN EL ACCESO O TRATAMIENTO POR PARTE DEL ENCARGADO**

El Responsable del Fichero o Tratamiento autoriza al Encargado de Tratamiento a tratar información de carácter personal contenida en los ficheros de su titularidad, única y exclusivamente, para \*\*\*\*\*

En Representación de la UNED,

En Representación de

Fdo.:

Fdo.:



## ANEXO 5.2.

### DEBER DE SECRETO Y PROHIBICIÓN DE ACCESO A DATOS PERSONALES

En cumplimiento de lo dispuesto en el artículo 83 del 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 , \*\*\*\*\*  
[INCLUIR LA DENOMINACIÓN SOCIAL, O, EN SU CASO, NOMBRE Y APELLIDOS DEL TERCERO PRESTADOR DE SERVICIOS], que presta los servicios de \*\*\*\* [INCLUIR LA CLASE DE SERVICIOS QUE PRESTA] a la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (en adelante, UNED) se compromete a que el personal designado para la prestación del citado servicio cumpla con las siguientes

### ESTIPULACIONES

#### **PRIMERA.- Del tratamiento de datos personales por parte de la UNED**

Los datos personales por ustedes facilitados, para los casos en que éste sea una persona física, o en el caso de representantes de una persona jurídica, serán incorporados a un fichero titularidad de la UNED.

La finalidad de la recogida y tratamiento de los mismos es el mantenimiento y gestión de la vinculación contractual establecida, el seguimiento de los servicios contratados, la facturación y la remisión de información sobre las incidencias relacionadas con los servicios prestados.

Asimismo, la UNED no cederá los datos personales de sus proveedores a terceros ajenos a esta Institución de Derecho Público, salvo en los supuestos legales en los que quede autorizada.

De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informo de su facultad para ejercer sus derechos de acceso, rectificación, cancelación y, en su caso, oposición, respecto de sus datos personales, dirigiendo o presentando al efecto un escrito, acompañado de fotocopia de su DNI, a la siguiente dirección:

UNED.....

## **SEGUNDA.- Prohibición de acceder a los datos de carácter personal de la UNED**

El personal de \*\*\*\*\* [INCLUIR LA DENOMINACIÓN SOCIAL, O, EN SU CASO, NOMBRE Y APELLIDOS DEL TERCERO PRESTADOR DE SERVICIOS], tiene prohibido el acceso a los datos personales, contenidos en los diferentes soportes, informático o en papel, así como a los recursos del sistema de información, para la realización del trabajo encomendado.

En caso de haber tenido acceso o conocimiento, directo o indirecto, de datos personales tratados en la UNED, estarán a lo dispuesto en la estipulación TERCERA del presente documento.

## **TERCERA.- Deber de secreto**

Si durante la realización del trabajo o prestación del servicio, el personal de \*\*\*\*\* [INCLUIR LA DENOMINACIÓN SOCIAL, O, EN SU CASO, NOMBRE Y APELLIDOS DEL TERCERO PRESTADOR DE SERVICIOS], hubiere tenido acceso o conocimiento, directo o indirecto, de datos de carácter personal tratados en la UNED, tendrá la obligación de mantener el deber de secreto respecto a su contenido, aun después de haber cesado su relación laboral o vínculo contractual con ésta.

Es obligación del prestador de servicios comunicar este deber a su personal, así como cuidar de su cumplimiento.

En el caso de que el personal de \*\*\*\*\* [INCLUIR LA DENOMINACIÓN SOCIAL, O, EN SU CASO, NOMBRE Y APELLIDOS DEL TERCERO PRESTADOR DE SERVICIOS], incumpla con el deber de secreto, efectuase una cesión o comunicación de los datos personales a terceros [entendiendo ésta como la revelación de datos personales a persona distinta del titular de los datos], o los utilizara para cualquier otro fin, a los efectos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, \*\*\*\*\* [INCLUIR LA DENOMINACIÓN SOCIAL, O, EN SU CASO, NOMBRE Y APELLIDOS DEL TERCERO PRESTADOR DE SERVICIOS], será considerado como Responsable de Fichero o Tratamiento, respondiendo así, de las infracciones previstas y fijadas en la citada norma.



**CUARTA.- Responsabilidad**

Ambas partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan de este documento, toda la legislación que resulte aplicable y especialmente, las obligaciones impuestas y determinadas por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normas de desarrollo. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento.

Por la UNED,

Por el Prestador de Servicios,

Fdo.:

Fdo.:

### ANEXO 6.1.

#### ACTUALIZACIÓN SEMESTRAL, del 1 de ..... al 30 de ..... de 20. DE LAS ACTIVIDADES Y TRATAMIENTO DE DATOS EN LAS DISTINTAS UNIDADES DE LA UNIVERSIDAD

Estimado/a compañero/a:

En aras de mantener actualizados los tratamientos de datos de carácter personal, tal como exige la normativa legal, te remito este cuestionario, como responsable de los ficheros de tu Unidad, para que a la mayor brevedad posible nos lo devuelvas cumplimentado.

1. ¿Has detectado algún tratamiento de datos nuevo?

2. ¿Se ha eliminado o desechado algún fichero íntegramente?

3. ¿Ha habido algún cambio en las personas que ejercen el cargo de gestor de fichero?

4. ¿Se han revisado, últimamente, las cláusulas LOPD que se incorporan a los impresos o formularios donde se recogen datos personales?

5. ¿Se han tramitado, conforme a la normativa, las solicitudes de ejercicio de los derechos ARCO?

6. ¿Se guardan o archivan documentos que contengan datos especialmente protegidos o sensibles, en esa Unidad?

7. En relación a las posibles incidencias de seguridad producidas en este periodo, ¿se han comunicado correctamente, siguiendo el procedimiento establecido?

8. ¿Propones alguna mejora de la protección de datos en la Universidad?

9. Existe algún aspecto que te preocupe en relación a la seguridad del contenido del fichero o ficheros, a tu cargo?

Te ruego que hagas la máxima difusión entre el personal adscrito a tu unidad y te agradezco tu colaboración en la protección de datos de carácter personal en la Universidad.

Jefa del Dpto. de Política Jurídica de  
Seguridad de la Información,

## ANEXO 6.2.

### SOLICITUD DE CREACIÓN DE FICHERO

#### DATOS DE LA PERSONA INTERESADA

D/ D<sup>a</sup> , cargo o puesto de trabajo   
 teléfono , e-mail de contacto   
 por medio del presente escrito,

#### SOLICITA (1),

La **creación** del fichero denominado , y que se inicien los trámites previstos en el art. 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el artículo 52 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la mencionada norma.

a  de  de 20

Firma de la persona solicitante

#### DEPARTAMENTO DE POLÍTICA JURÍDICA DE SEGURIDAD DE LA INFORMACIÓN

**Presentar cumplimentado el siguiente cuestionario. Remitirlo como documento adjunto a la siguiente dirección: [incidenciaslopd@adm.uned.es](mailto:incidenciaslopd@adm.uned.es)**

**SOLICITUD DE CREACIÓN DE FICHERO****IDENTIFICACIÓN DE LA PERSONA DE LA UNED QUE CUMPLIMENTA EL PRESENTE FORMULARIO**

Nombre y Apellidos

Área a la que pertenece

Cargo o puesto

Fecha

**Notas.-**

- Este formulario permite la cumplimentación electrónica.
- Lea asimismo las 'Notas' de los diferentes apartados, a los efectos de marcar las casillas correspondientes.
- Recuerde que ha de cumplimentar este formulario, por cada una de los ficheros que identifique.

## 1. NOMBRE DEL FICHERO

## 2.- DESCRIPCIÓN DE LA FINALIDAD DEL FICHERO Y USOS PREVISTOS

**Nota.-** En primer lugar, indique, mediante texto libre, una descripción de la finalidad y usos previstos para el fichero.

A continuación, de acuerdo con la tipificación prevista por la Agencia Española de Protección de Datos, marque las casillas correspondientes a la finalidad y usos previstos del fichero.

### FINALIDADES

**ATENCIÓN.-** Sólo podrá marcar hasta un máximo de 6 casillas, de modo que señale las finalidades y usos más aproximados a la realidad, esto es, los más necesarios u obligatorios.

<input type="checkbox"/> <b>Recursos Humanos</b>
Gestión de Personal Formación de Personal Acción Social a favor del personal de las administraciones públicas Promoción y selección de personal Oposiciones y concursos Control horario Control de patrimonio de altos cargos Control de incompatibilidades

**Gestión de Nómina**

**Prevención de riesgos laborales**

**Hacienda pública y gestión de la administración tributaria**

<input type="checkbox"/> <b>Gestión económica-financiera pública</b>
Gestión de deuda pública Gestión financiera pública Gestión de catastros inmobiliarios rústicos y urbanos Relaciones comerciales con el exterior Regulación de mercados financieros Defensa de la competencia

<input type="checkbox"/> <b>Gestión contable, fiscal y administrativa</b>
Gestión económica y contable Gestión de facturación y gestión fiscal

<input type="checkbox"/> <b>Justicia</b>
Procedimientos judiciales Registros vinculados con la fe pública Tramitación de indultos

<input type="checkbox"/> <b>Seguridad pública y defensa</b>
Protección civil Seguridad vial Actuaciones de fuerzas y cuerpos de seguridad con fines administrativos Gestión y control de centros e instituciones penitenciarias Solicitudes de visado/residencia

<input type="checkbox"/> <b>Actuaciones de fuerzas y cuerpos de seguridad con fines policiales</b>
--

**Video vigilancia**

<input type="checkbox"/> <b>Trabajo y gestión de empleo</b>
Promoción y gestión de empleo Relaciones laborales y condiciones de trabajo Inspección y control de seguridad social Formación profesional ocupacional Prestaciones a desempleados Prestaciones de garantía salarial Prestaciones a desempleados Prestaciones de garantía salarial

<input type="checkbox"/> <b>Servicios sociales</b>
Prestaciones de asistencia social Inspección de protección social Pensiones, subsidios y otras prestaciones económicas Acción a favor de Inmigrantes Servicios sociales a minusválidos Servicios sociales a la tercera edad Promoción social a la mujer Promoción social a la juventud Protección del menor Acción a favor de toxicómanos, ayudas acceso a la vivienda y otros servicios sociales

**Gestión y control sanitario**

Gestión sanitaria  
Control sanitario  
Gestión de tarjeta sanitaria

 **Historial clínico**
 **Investigación epidemiológica y actividades análogas**
 **Educación y cultura**

Enseñanza  
Educación especial  
Becas y ayudas a estudiantes  
Fomento y apoyo a actividades artísticas y culturales  
Protección del patrimonio histórico-artístico

 **Función Estadística Pública**
 **Padrón de Habitantes**
 **Gestión de Censo Poblacional**
 **Fines Históricos, estadísticos y científicos**

Fines históricos  
Encuestas sociológicas o de opinión  
Fines estadísticos no amparados en la legislación estatal o autonómica  
Fines científicos

 **Seguridad y control de acceso a edificios**
 **Procedimientos administrativos**

Gestión de procedimientos administrativos  
Registros de entrada/salida de documentos  
Otros registros administrativos  
Atención al ciudadano  
Concesión y gestión de premisos  
Licencias y autorizaciones

 **Publicaciones**
 **Gestión sancionadora**
 **Prestación de Servicios de Certificación Electrónica**
 **Otras finalidades**

### 3. SISTEMA DE TRATAMIENTO

**Nota.-** En este apartado deberá indicar el sistema utilizado para tratar la información de carácter personal. En la práctica, es frecuente que los datos sean tratados a través de una aplicación informática y, a su vez, se encuentren también en un archivo en papel – con el cual tiene correlación -. De modo que, podemos encontrar que el sistema de tratamiento es Mixto. Señale a continuación, cual es entonces el sistema de tratamiento empleado.

- Automatizado [Informático]  
 Manual [Sólo Papel]  
 Mixto [Informático y Papel]

En caso de tener un tratamiento SÓLO AUTOMATIZADO, indique la aplicación informática empleada para tales efectos.

- Excel  
 Access  
 Word  
 Otros [indicar en el recuadro el nombre del programa o aplicación informática]

### 4. ORIGEN Y PROCEDENCIA DE LOS DATOS

#### Origen

- El propio interesado o su representante legal  
 Otras personas físicas  
 Fuentes accesibles al público [Ver Glosario de Términos]  
 Registros públicos  
 Administraciones Públicas

#### Colectivos o categorías de interesados

**ATENCIÓN.-** Sólo puede marcar hasta un máximo de 6 casillas, de modo que señale sólo aquéllos colectivos de los que sea necesaria u obligatoria la recogida y tratamiento de datos.

- Empleados  
 Ciudadanos y residentes  
 Contribuyentes y sujetos obligados  
 Proveedores  
 Asociados o miembros

- Propietarios o arrendatarios
- Pacientes
- Estudiantes
- Representantes legales
- Personas de contacto
- Solicitantes
- Beneficiarios
- Inmigrantes
- Demandantes de empleo
- Cargos públicos

Otros colectivos

## 5. TIPOS DE DATOS, ESTRUCTURA Y ORGANIZACIÓN DEL FICHERO

**Nota.-** Señale que tipo de datos de carácter personal son objeto de tratamiento.

### Datos especialmente protegidos

- Ideología
- Afiliación sindical
- Religión
- Creencias
- Origen racial o étnico
- Salud
- Vida sexual

### Relativos a la comisión de infracciones penales o administrativas

- Datos relativos a infracciones penales
- Datos relativos a infracciones administrativas

### Datos de carácter identificativo

- NIF/DNI
- Nombre y apellidos
- Nº Registro de personal
- Marcas físicas
- Tarjeta Sanitaria
- Firma electrónica
- Teléfono [Fijo y/o Móvil]
- Nº SS / Mutualidad
- Imagen / voz

- Dirección [Postal y/o Correo electrónico]  
 Firma/huella

**OTRO TIPO DE DATOS** [Marque las casillas correspondientes a la categoría de datos personales objeto de tratamiento]

- CARACTERÍSTICAS PERSONALES** [Datos de estado civil; Edad; Datos de familia; Sexo; Fecha de nacimiento; Nacionalidad; Lugar de nacimiento; Lengua materna]
- DATOS DE CIRCUNSTANCIAS SOCIALES** [Características de alojamiento, vivienda; Situación militar; Propiedades, posesiones; Aficiones y estilo de vida; Pertinencia a clubes, asociaciones; Licencias, permisos, autorizaciones].
- DATOS ACADÉMICOS Y PROFESIONALES** [Formación; Titulaciones; Historial de estudiante; Experiencia profesional; Pertinencia a colegios o asociaciones profesionales]
- DATOS DETALLE DE EMPLEO** [Cuerpo/Escala; Categoría/grado; Puestos de trabajo; Datos no económicos de nómina; Historial del trabajador]
- DATOS DE INFORMACIÓN COMERCIAL** [Actividades y negocios; Creaciones artísticas, literarias, científicas o técnicas; Licencias comerciales; Suscripciones a publicaciones/medios de comunicación]
- DATOS ECONÓMICO-FINANCIEROS Y DE SEGUROS** [Ingresos, rentas; Inversiones, bienes patrimoniales; Créditos, préstamos, avales; Datos bancarios; Planes de pensiones, jubilación; Datos económicos de nómina; Datos deducciones impositivas/impuestas; Seguros; Hipotecas; Subsidios, beneficios; historial créditos; Tarjetas crédito]
- DATOS DE TRANSACCIONES** [Bienes y servicios suministrados por el afectado; Bienes y servicios recibidos por el afectado; Transacciones financieras; Compensaciones/indemnizaciones]
- OTRO TIPO DE DATOS** [Indicar en el recuadro]

## 6. CESIÓN O COMUNICACIÓN DE DATOS

**Nota.-** Este apartado únicamente ha de cumplimentarse en el caso de que se prevea realizar cesiones o comunicaciones de datos. No se considerará cesión de datos la prestación de un servicio al Responsable del Fichero por parte del Encargado del Tratamiento. La comunicación de los datos ha de ampararse en alguno de los supuestos legales establecidos en la LOPD.

### Categorías o destinatarios de cesiones

**ATENCIÓN.-** Sólo puede marcar hasta un máximo de 6 casillas, de modo que señale sólo aquéllas categorías o destinatarios de cesiones [cesionarios].

- Organismos de la seguridad social
- Hacienda pública y administración tributaria
- Instituto Nacional de Estadística
- Registro públicos
- Órganos judiciales
- Tribunal de cuentas o equivalente autonómico
- Órganos de la Unión Europea
- Otros órganos de la Administración del Estado
- Otros órganos de la Comunidad Autónoma
- Diputaciones provinciales
- Otros órganos de la administración local
- Sindicatos y juntas de personal
- Colegios profesionales
- Cámaras de la propiedad
- Cámaras de comercio industria y navegación
- Notarios, Abogados, Procuradores
- Clubes deportivos y federaciones
- Organizaciones y asociaciones sin ánimo de lucro
- Fuerzas y cuerpos de seguridad
- Bancos, Cajas de ahorro y cajas rurales
- Entidades aseguradoras
- Otras entidades financieras
- Entidades Sanitarias
- Interesados legítimos
- Otros [Indicar en el recuadro]

## ANEXO 6.3.

## SOLICITUD DE MODIFICACIÓN DE FICHERO

## DATOS DE LA PERSONA INTERESADA

D/D<sup>a</sup> , cargo o puesto de trabajo , teléfono , e-mail de  contacto por medio del presente escrito,

## SOLICITA (1),

La **modificación** del fichero denominado  y que se inicien los trámites previstos en el art. 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el artículo 52 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la mencionada norma.

a  de  de 20

## Firma de la persona solicitante



## DEPARTAMENTO DE POLÍTICA JURÍDICA DE SEGURIDAD DE LA INFORMACIÓN

**Presentar cumplimentado el siguiente cuestionario. Remitirlo como documento adjunto a la siguiente dirección: [incidenciaslopd@adm.uned.es](mailto:incidenciaslopd@adm.uned.es)**

<b>CUESTIONARIO</b>
---------------------

Cumplimentar sólo los apartados que sean objeto de modificación

- 1.- Nombre del fichero:**
- 2.- Responsable del fichero:**
- 3.- Descripción del fichero:**
- 4.- Encargado del tratamiento:**
- 5.- Campos del fichero:**
- 6.- Finalidad y usos previstos:**
- 7.- Personas o colectivos sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos:**
- 8.- Procedencia y procedimientos de recogida de datos:**
- 9.- Cesiones:**
- 10.- Transferencia internacional de datos:**
- 11.- Medidas de seguridad:**
- 12.- Sistema de tratamiento:**
- 13.- Observaciones:**

## INSTRUCCIONES DE CUMPLIMENTACIÓN

- 1.- **Nombre del fichero:** Se indicará la denominación que se propone.
- 2.- **Responsable del fichero:** Órgano responsable del mismo.
- 3.- **Descripción del fichero:** Se indicará una breve descripción del contenido del fichero.
- 4.- **Encargado del tratamiento:** Sólo se cumplimentará cuando terceros traten datos personales por cuenta del responsable del tratamiento. No se considera encargado del tratamiento a la persona física que tenga acceso a los datos personales en su condición de empleado dentro de la relación laboral que mantiene con el responsable del fichero.  
**Se indicarán los datos del tercero o terceros, si son varios:** Nombre, NIF o CIF, actividad principal, dirección o razón social y objeto del contrato de prestación suscrito con la UNED.
- 5.- **Campos del fichero:** Se especificarán los datos que contiene, nombre, apellidos,...
- 6.- **Finalidad y usos previstos:** Se detallará la finalidad por una parte y los usos previstos por otra.
- 7.- **Personas o colectivos sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos.**
- 8.- **Procedencia y procedimientos de recogida de datos:** Se especificará la procedencia por una parte y los procedimientos de recogida por otra.  
  
En lo que respecta a la procedencia, deberá indicarse si proceden del interesado o representante legal, otras personas físicas o jurídicas, fuentes accesibles al público, registros públicos y administraciones públicas, según sea el caso.  
  
En lo que respecta a los procedimientos de recogida, se especificará si proceden de formularios o solicitudes, de encuestas y entrevistas, de transmisión por Internet, por vía electrónica u otros (indicar en este último caso cuáles), según corresponda.  
  
Se indicará el soporte utilizado, papel, informático, vía telemática u otros e indicar en este último caso cuáles.
- 9.- **Cesiones:** Sólo se cumplimentará en el caso de que la comunicación o la transmisión de los datos se realice a persona distinta de su titular.
- 10.- **Transferencia internacional de datos:** Sólo se cumplimentará si existe una transferencia de datos a otros países.

**11.- Medidas de seguridad.** Se indicará el nivel de seguridad del fichero, teniendo en cuenta lo siguiente:

- Nivel **alto**: datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Nivel **medio**: datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, servicios de solvencia patrimonial y crédito y aquellos que permitan obtener una evaluación de la personalidad del individuo.
- Nivel **básico**: los demás datos.

**12.- Sistemas de tratamiento:** Se especificará, de forma concisa, si el tratamiento es automatizado, no automatizado o en soporte papel o mixto.

**13.- Observaciones:**

## ANEXO 6.4.

## SOLICITUD DE SUPRESIÓN DE FICHERO

## DATOS DE LA PERSONA INTERESADA

D/ D<sup>a</sup>  cargo o  
 puesto de trabajo  teléfono  
 e-mail de contacto  por medio del presente  
 escrito,

## SOLICITA (1),

La **supresión** del fichero denominado  y que se  
 inicien los trámites previstos en el art. 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de  
 Protección de Datos de Carácter Personal, y en el artículo 52 del Real Decreto 1720/2007, de 21  
 de diciembre, por el que se desarrolla la mencionada norma.

El motivo o causa de la **supresión** sería

En caso de producirse la supresión del fichero, el **destino** de la información contenida en  
 él sería

a  de  de 20

Firma de la persona solicitante

## DEPARTAMENTO DE POLÍTICA JURÍDICA DE SEGURIDAD DE LA INFORMACIÓN

Presentar cumplimentado el siguiente cuestionario. Remitirlo como documento

adjunto a la siguiente dirección: [incidenciaslopd@adm.uned.es](mailto:incidenciaslopd@adm.uned.es)

### ANEXO 7.1.

Este Rectorado, en uso de las atribuciones conferidas por el artículo 99 v) de los Estatutos de la Universidad y los artículos 10 y 29 del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, ha resuelto nombrar a los miembros del Comité de Seguridad de la Información de la UNED y la función a desempeñar en el mismo.

Responsable de la Información	Presidente del Comité
Responsable de la Seguridad de la Información	Vocal
Responsable del Servicio	Vocal
Responsable del Sistema	Vocal
Director del CTU	Vocal
Secretaria General o persona en quien delegue	Vocal
Jefa del Departamento de Política Jurídica de Seguridad de la Información	Vocal
Administrador de la Seguridad del Sistema	Vocal
Asesor de Seguridad	Asesor (con voz y sin voto)
Jefa de la Sección de Protección de Datos	Secretaria del Comité (con voz y sin voto)

Sin perjuicio de la asistencia de los miembros antes citados, podrán asistir otros cargos o técnicos de la Universidad al Comité de Seguridad de la Información, cuando se trate de temas relacionados con el Esquema Nacional de Seguridad.

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

EL RECTOR,

Fdo.: .....

## ANEXO 7.2.

Este Rectorado, en uso de las atribuciones conferidas por el artículo 99 v) de los Estatutos de la Universidad y de la regulación de los artículos 95 y 109 del R.D. 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, ha resuelto nombrar al **Director del CTU** como Responsable de Seguridad de los ficheros automatizados de la Universidad en materia de protección de datos.

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

El RECTOR,

Fdo.: .....

## ANEXO 8.1.

### Modelo de Formulario de presentación de sugerencias, quejas o reclamaciones

Comunicación de sugerencias, quejas o reclamaciones relativas a la aplicación del “Código Tipo en materia de Protección de Datos de la Universidad Nacional de Educación a Distancia (UNED)”

#### Datos del solicitante:

D./D<sup>a</sup> ..... mayor de edad, con domicilio en ..... nº..... Localidad..... Provincia..... Código Postal..... teléfono..... e-mail..... con DNI nº..... del que se acompaña fotocopia, por medio del presente formulario manifiesta su deseo de ejercer su derecho de presentación de sugerencias, quejas o reclamaciones, de conformidad con el Código de Conducta de la UNED

#### Expone:

1. Que ha tenido conocimiento de los siguientes hechos en relación al tratamiento de datos de carácter personal sometidos al “Código Tipo en materia de protección de datos de la UNED”

.....  
.....  
.....  
.....

2. Que interesa que se constate la certeza de los hechos expuestos y, en su caso, se proceda a la rectificación de las actuaciones a que a los mismos hacen referencia. Asimismo, que se me notifique la resolución que se adopte.

En ..... a ..... de ..... De 20.....

Fdo.:

**Sr. Presidente de la Comisión de Control del Código Tipo**

## ANEXO 9

### ENCUESTA DE SATISFACCIÓN DEL SERVICIO DE LA SECCIÓN DE PROTECCIÓN DE DATOS DE LA UNED

Agradeciendo de antemano su colaboración, le rogamos cumplimente este breve cuestionario que nos servirá para mejorar nuestros servicios.

**1. Valore, por favor, el plazo de atención de su solicitud:**

Excelente       Bueno       Normal       Malo

**2. Indique cómo calificaría la atención recibida por el personal de la Sección:**

Excelente       Bueno       Normal       Malo

**3. Valore la celeridad con que se ha resuelto su solicitud:**

Excelente       Bueno       Normal       Malo

**4. Su grado de satisfacción con la resolución dada es:**

Excelente       Bueno       Normal       Malo

**5. Satisfacción general con el servicio:**

Muy buena       Buena       Aceptable       Mejorable

**6. Observaciones y/o sugerencias para la mejora:**



## ANEXO 10.1.

El próximo 28 de enero, se celebra el Día de Protección de Datos en Europa; una jornada impulsada por la Comisión Europea, el Consejo de Europa y las autoridades de protección de datos de los Estados miembros de la UE.

El objetivo principal de este día de celebración, es impulsar entre los ciudadanos el conocimiento de sus derechos y obligaciones en materia de protección de datos.

Por ello la UNED, a través del Departamento de Política Jurídica de Seguridad y Protección de Datos difunde información, normativa, modelos de documentos y buenas prácticas sobre protección de datos desde su página Web:

[http://portal.uned.es/portal/page?\\_pageid=93,1049794&\\_dad=portal&\\_schema=PORTAL](http://portal.uned.es/portal/page?_pageid=93,1049794&_dad=portal&_schema=PORTAL)



## ANEXO 10.2.

### COMUNICADO SOBRE DESECHADO Y DESTRUCCIÓN DE DOCUMENTOS EN PAPEL

Estimada/o compañera/o:

Como responsable de un fichero de datos de carácter personal o de una Unidad de gestión de la UNED, es importante que conozcas las exigencias de la normativa vigente en materia de protección de datos sobre el tratamiento de datos de carácter personal en soporte papel o automatizado y las obligaciones que como usuario debes cumplir.

El Real Decreto 1720/2007 que desarrolla la LOPD, en su artículo 92.4 señala lo siguiente: *“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 contenido en el mismo o su recuperación posterior”*.

En este sentido se puede señalar que existen, en todos los edificios de la Universidad, cajas de cartón distribuidas por pasillos, zonas de fotocopiadoras y zonas comunes. **El papel que se deposita en las cajas** se retira para su reciclaje, pero **no se destruye**. Se ha detectado que en estas cajas se depositan documentos o papeles que contienen datos de carácter personal que, en cumplimiento de la normativa de protección de datos, deberían ser destruidos.

Por lo que se recuerda que si la documentación que se va a tirar contiene datos personales, **NO DEBE depositarse** en dichas cajas. En estos casos será eliminada por una máquina destructora o bien se remitirá un correo electrónico al departamento de Servicios Generales que se encargará de su retirada, destrucción certificada y posterior reciclaje.

Así mismo, aprovecho para enviarte el enlace al Espacio de protección de datos de la Web UNED, en el que podrás encontrar información de utilidad.



Para cualquier consulta, en materia de protección de datos, dispones de la siguiente dirección: [dptojuridicoseguridad@adm.uned.es](mailto:dptojuridicoseguridad@adm.uned.es)

Te ruego que hagas la máxima difusión entre el personal adscrito a tu unidad agradeciendo tu participación en la protección a los datos de carácter personal.

Un saludo.