CÓDIGO DE CONDUCTA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED)

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

Adaptado al Reglamento Europeo 2016/679, 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 ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Aprobada, su adaptación, por el Consejo de Gobierno de la UNED el 30 de abril de 2019

Universidad Nacional de Educación a Distancia
c/ Bravo Murillo, 38
28015 Madrid

ÍNDICE

INTRODUCCIÓN 4

1. OBJETIVO DEL CÓDIGO DE CONDUCTA 4

2. CONTENIDO DEL CÓDIGO DE CONDUCTA 5

2.1. MARCO NORMATIVO 5

2.2. DEFINICIONES 6

2.3. ÁMBITO DE APLICACIÓN 9

2.4. ENTRADA EN VIGOR 9

2.5. OBLIGACIONES POSTERIORES A LA INSCRIPCIÓN DEL CÓDIGO DE CONDUCTA 9

2.6. PRINCIPIOS DE LA PROTECCIÓN DE DATOS 10

2.6.1. Principios relativos al tratamiento 10

2.6.2. Deber de información en la recogida de datos 11

2.6.3. Licitud de los tratamientos 12

2.6.4. Principio de seguridad de los datos 12

2.6.5. El deber de secreto en el tratamiento de datos 13

2.6.6. Datos de categorías especiales (especialmente protegidos) 13

2.6.7. Comunicación de datos 14

2.6.8. Las transferencias internacionales de datos 16

2.6.9. Los Encargados de tratamiento 16

2.7. DERECHOS DEL INTERESADO 18

2.7.1. Consideraciones generales 18

2.7.2. El derecho de acceso 19

2.7.3. El derecho de rectificación 21

2.7.4. Derecho de supresión 21

2.7.5. Derecho de oposición 22

2.7.6. Derecho de limitación del tratamiento 24

2.7.7. Derecho a la portabilidad 25

2.8. ACCIONES FORMATIVAS EN MATERIA DE PROTECCIÓN DE DATOS 25

2.9. REGISTRO DE ACTIVIDADES DE TRATAMIENTO 26

2.9.1. Registro de actividades como Responsable 26

2.9.2. Registro de actividades como Encargado de Tratamiento 26

2.10. MEDIDAS DE RESPONSABILIDAD PROACTIVA 27
2.10.1. Responsabilidad Proactiva 27
2.10.2. Protección de datos desde el diseño y por defecto 27
2.10.3. Medidas de seguridad 28
2.10.4. Notificación de violaciones de seguridad 28
2.11. ROLES Y RESPONSABILIDADES 29
2.12. LA COMISIÓN DE CONTROL DEL CÓDIGO DE CONDUCTA 30
2.13. PRESENTACIÓN DE SUGERENCIAS, QUEJAS O RECLAMACIONES 31
2.14. INFRACCIONES Y SANCIONES 32
2.15. PROCEDIMIENTO SANCIONADOR 32
2.16. DIFUSIÓN Y EVALUACIÓN DE SATISFACCIÓN 33
2.17. MEMORIA DE ACTIVIDADES 34
ANEXOS

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 171.000 estudiantes que cursan sus titulaciones oficiales (28 grados, 75 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 DE CONDUCTA

Los códigos de conducta 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 de Conducta 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 los artículos 40 y ss. del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) – en adelante RGPD- y a los artículos 38 y 39 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y por la que se deroga la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, la UNED pretende disponer de un Código de Conducta 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 el RGPD.

Debemos tener en cuenta que el Código de Conducta 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 de Conducta está redactado en términos claros y accesibles y desarrollará, como mínimo, los aspectos que se relacionan a continuación:

- El tratamiento leal y transparente.
- Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos.
- La recogida de datos personales.
- La información proporcionada al público y a los interesados.
- El ejercicio de los derechos de los interesados.
- Las medidas y procedimientos para garantizar la protección de datos desde el diseño y por defecto.
- Las medidas para garantizar la seguridad del tratamiento.
- La notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados.
- La transferencia de datos personales a terceros países u organizaciones internacionales.

En particular contiene el Código:

- Cláusula 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, en la recogida de datos.
- Formulario para el ejercicio, por los afectados, de sus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento de 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.
- La Política de Seguridad de la Información.
- La Normativa y los procedimientos relacionados con la seguridad y la protección de datos personales.

2. CONTENIDO DEL CÓDIGO DE CONDUCTA

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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- Artículo 3
- Artículo 6
- Artículo 133
- Artículo 346
- Disposición adicional decimoquinta
- Disposición adicional decimosexta
- Disposición adicional vigésima quinta

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, modificada por Ley 18/2015, de 9 de julio.
- 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
- 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
- Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED, aprobado en Consejo de Gobierno de 12 de diciembre de 2017

2.2. DEFINICIONES

- **Bloqueo de datos:** El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos.

- **Comité de Seguridad de la Información:** se encargará de coordinar y centralizar la gestión tecnológica en materia de seguridad, que será competencia de la Gerencia de la Universidad y del Centro de Tecnología de la UNED (CTU). Al Comité le corresponde aplicar, en el ámbito de la UNED, las previsiones contenidas en el ENS y determinar la Política de Seguridad que se ha de emplear en la utilización de los medios electrónicos que permitan la adecuada protección de la información.
- **Consejo de Gobierno**: es el órgano colegiado de gobierno de la Universidad al que corresponde establecer sus líneas estratégicas y programáticas, así como las directrices y procedimientos para su aplicación en los ámbitos de organización de las enseñanzas, investigación, recursos humanos y económicos y elaboración de los presupuestos, y ejerce las funciones previstas en la Ley Orgánica de Universidades, y en estos estatutos.
- **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.
- **Datos biométricos**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.
- **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.
- **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.
- **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. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines 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.
- **Fichero**: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- Fichero Temporal: Ficheros de trabajo creados por usuarios o procesos necesarios para un tratamiento ocasional, o como paso intermedio para la realización de un tratamiento

- **Gerente**: bajo la dependencia del Rector, es el responsable de la gestión de los servicios administrativos y económicos de la Universidad.
- **Limitación del tratamiento**: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
- **Personal de administración y servicios (PAS)**: El personal de administración y servicios de la UNED está integrado por funcionarios de escalas propias y personal laboral de los grupos propios de esta Universidad, así como por funcionarios de carrera y personal laboral fijo pertenecientes a cuerpos, escalas y grupos de otras Administraciones públicas, que presten servicios en esta Universidad. Le corresponde la gestión y administración, así como el apoyo, asistencia y asesoramiento a las autoridades académicas en las áreas de recursos humanos, asuntos económicos, biblioteca, archivo, servicios informáticos, producción y distribución de medios impresos y audiovisuales, servicios generales y cualesquiera otros procesos de gestión administrativa, técnica y de soporte a la docencia y a la investigación que se determinen necesarios para la Universidad en el cumplimiento de sus fines.
- **Personal Docente e Investigador (PDI):** El personal docente e investigador de la UNED está compuesto por funcionarios de los cuerpos docentes universitarios y por personal contratado. Asimismo tendrán la consideración de personal docente e investigador en formación los becarios que colaboren en tareas de docencia o investigación
- **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; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.
- **Servicio de inspección**: La UNED cuenta con un Servicio de Inspección para contribuir 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
- **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 la autoridad directa del responsable o del encargado.
- **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.
- **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.

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 de Conducta entrará en vigor y será plenamente eficaz a partir de la fecha de la aprobación del mismo por 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 de Conducta, 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 DE CONDUCTA

- 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 de Conducta, los procedimientos de adhesión, en su caso, y de garantía de su cumplimiento y la relación de adheridos, si los hubiera. 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 de Conducta, 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 de Conducta, por la Comisión de control del Código, 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. Su incumplimiento puede suponer una lesión del derecho fundamental a la protección de datos de carácter personal.

2.6.1. Principios relativos al tratamiento

Estos principios establecen una serie de fundamentos, por los que deben ser recogidos y tratados los datos personales en la Universidad:

Licitud, lealtad y transparencia. Para ello se tienen en cuenta los siguientes apartados:

- Se tiene el consentimiento para cada finalidad del tratamiento
- Se informa con carácter previo a recabar el consentimiento
- Existe una obligación legal para el tratamiento
- El tratamiento es necesario para ejecutar un contrato o precontrato
- El tratamiento es necesario para el cumplimiento de interés público

Limitación de la finalidad, exactitud de los datos:

- Los datos personales se recogen con fines determinados y explícitos
- Los datos solo se tratan ulteriormente de manera compatible con otros fines
- Los datos personales se mantienen exactos y actualizados
- Se rectifican los datos inexactos

Minimización de datos

- Para la prestación de un servicio o ejecución de un contrato se solicitan sólo los datos necesarios.

Limitación del plazo de conservación de los datos

- Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran

derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación, asimismo, lo dispuesto en la Normativa de archivos y documentación.

Integridad y confidencialidad

- Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos.
- Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos.
- Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental.

Responsabilidad Proactiva

El Responsable del tratamiento es el encargado del cumplimiento de lo dispuesto en los apartados anteriores y debe ser capaz de demostrarlo.

2.6.2. Deber 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, el RGPD establece a la vez un derecho para el ciudadano y un deber para el Responsable del Tratamiento. 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 Tratamiento tiene la obligación de informar al interesado, cuyos datos van a ser tratados, en los términos regulados en los artículos 13 y 14 del RGPD, acerca de lo siguiente:

- La identidad y los datos de contacto del responsable y, en su caso, de su representante.
- Los datos de contacto del delegado de protección de datos.
- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- Cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero.
- Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
- En su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

Esta información está contemplada, de forma legible y con fácil acceso, en los formularios o cuestionarios en papel o electrónicos (Internet), que se utilizan para recoger los datos. Ver el punto 2 “Cumplimiento del deber de Información”, de los Anexos de este Código.

Este derecho de información es esencial porque condiciona el ejercicio de otros derechos tales como el derecho de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, que se exponen a continuación.

Este derecho de información es esencial porque condiciona el ejercicio de otros derechos tales como el derecho de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, que se exponen en el punto 2.7. de este Código.

2.6.3. Licitud de los tratamientos

El tratamiento solo será lícito si puede enmarcarse dentro de alguna de las siguientes condiciones:

a) El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos

b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento

d) El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En el momento de recoger los datos de los interesados, en las cláusulas informativas elaboradas al efecto, se incluye la base legal sobre la que se desarrolla el tratamiento. Asimismo, en el Registro de Actividades de Tratamiento se identifican las bases legales aplicables en cada caso concreto.

2.6.4. Principio de seguridad de los datos

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

Las medidas de seguridad se adoptan 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.

El Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED (ANEXO 4.1.) prevé las medidas de seguridad tanto para los tratamientos automatizados, como para los no automatizados (en papel).

2.6.5. El deber de secreto en el tratamiento de datos

El Responsable del Tratamiento 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 Responsable del Tratamiento.

Teniendo en cuenta estas circunstancias, el Responsable del Tratamiento 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.
- 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.
- Firmar compromisos de confidencialidad con todos los usuarios de los sistemas de información con acceso a datos de carácter personal.

Para el cumplimiento de estas medidas el Consejo de Gobierno de la Universidad aprobó el Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED (ANEXO 4.1.), donde se señalan las obligaciones de los usuarios de la Universidad con acceso a datos personales, fijando las pautas de seguridad del uso del Sistema de Información así como las consecuencias de su incumplimiento.

2.6.6. Datos de categorías especiales (especialmente protegidos)

Los datos especialmente protegidos son aquellos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

La UNED trata datos especialmente protegidos, debido a que, principalmente, se recaban datos de salud. Tal es el caso de los tratamientos de: Becas al estudiante, Gestión de investigación, Prevención de riesgos laborales, Igualdad y Acción Social, Estudiantes con discapacidad (UNIDIS), Servicio de Inspección y Servicio de Psicología Aplicada.

Como norma general queda prohibido el tratamiento con datos especialmente protegidos, salvo que dicho tratamiento entre en alguno de los siguientes supuestos:

a) El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados. A fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias y origen racial o étnico.

b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social.

c) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

d) El tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.

e) El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.

f) El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

g) El tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. Deberá estar amparado en una norma con rango de ley.

h) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1 del RGPD, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

2.6.7. Comunicación de datos

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 y Formación Profesional
    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

2.6.8. Las transferencias internacionales de datos

Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo, en los términos del RGPD y, en concreto, de los artículos 45, 47 y 49.

- A países, territorios u organizaciones internacionales sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado.
- Cuando se hayan ofrecido garantías adecuadas sobre la protección, que los datos recibirán en su destino.
- Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

Fuera de estos supuestos se deberá obtener autorización previa del Director de la Agencia Española de Protección de Datos.

Actualmente, en la UNED, únicamente están previstas las Transferencias Internacionales de datos relacionadas a continuación:

1. Respecto a la información contenida en el tratamiento 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 tratamiento 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, solicitado por la Uned , emitido por la AEPD con fecha 18 de diciembre de 2015 y el convenio suscrito entre la UNED y Microsoft Ibérica, sobre OFFICE 365, se ha previsto el tratamiento de "Gestión del correo dominio uned.es en la Nube", en el que consta la transferencia internacional de datos a Estados Unidos.

4. En el tratamiento de la Gestión de Investigación: a México y Colombia contando con el consentimiento inequívoco, previo, del interesado en cada caso.

2.6.9. Los Encargados de tratamiento

El artículo 28 del RGPD señala 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.

- Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

- El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

  a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.
  b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
  c) tomará todas las medidas necesarias de conformidad con el artículo 32.
  d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento.
  e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III.
  f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.
  g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros.
  h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

- El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y

organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado. (La adhesión del encargado del tratamiento a un código de conducta o a un mecanismo de certificación podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes)

Actualmente en la UNED, los contratos en ejecución con tratamiento de datos personales tienen las siguientes finalidades:

- Mantenimiento y soporte de aplicaciones informáticas (bolsa empleo, participación de estudiantes).
- Mantenimiento de la enseñanza virtual de la UNED.
- Mantenimiento de la plataforma de la gestión académica del alumnado.
- Impresión de los títulos universitarios.
- Guarda y custodia de la documentación del Archivo General.
- Servicio de mensajería.
- Servicio de fotografía profesional.
- Mantenimiento de los relojes de control horario.
- Soporte de la gestión económica y de Recursos Humanos.
- Distribución y ventas de la Editorial UNED.

2.7. DERECHOS DEL INTERESADO

El derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos.

Entre los derechos que la Ley otorga a los interesados en relación con sus datos personales están los derechos de acceso, rectificación, supresión (derecho al olvido), oposición, portabilidad y limitación del tratamiento.

Éste constituye uno de los aspectos más importantes de la legislación relativa a la protección de datos de carácter personal, dado que un mal conocimiento o mala gestión del procedimiento de ejercicio de derechos suele ser la antesala de un posible procedimiento sancionador. Por ello, la UNED informa sobre el derecho fundamental a la protección de datos, 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 normativa vigente, garantizando así el derecho a la protección de datos.

2.7.1. Consideraciones generales

El RGPD no sólo modifica el catálogo de derechos, sino que además introduce novedades en el procedimiento para su ejercicio.

- Se ha de aplicar en todo momento el **Principio de Transparencia**. Toda la información que se dirija al interesado ha de ser concisa, de fácil acceso y a través de un lenguaje claro y sencillo.

- Los responsables deben **facilitar a los interesados el ejercicio de sus derechos**. Este mandado contenido en el artículo 12.2 del RGPD supone que los procedimientos y las formas que se faciliten a los interesados, para el ejercicio de sus derechos, deben ser visibles, accesibles y sencillos.

- **Se establece como una obligación** expresa de los responsables hacer efectivos los derechos del interesado.

- El ejercicio de los derechos será **gratuito** para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas.

- El modo en el cual debe ejercitar el afectado los derechos viene determinado por su **carácter de personalísimo**, pudiendo ejercerse por representante legal o voluntario, siempre que se acredite tal representación.

- Se trata de **derechos independientes**, es decir, que el ejercicio de ninguno de ellos es requisito previo para el ejercicio del otro.

- El responsable que trate una **gran cantidad de información** sobre un interesado podrá pedir a éste que especifique la información a que se refiere su solicitud de acceso.

- El responsable podrá contar con la **colaboración de los encargados** para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.

- Ante la solicitud de ejercicio de derechos el responsable deberá informar al interesado sobre las actuaciones derivadas de su petición en el **plazo de un mes,** artículo 12.3 RGPD. Este plazo podrá **extenderse dos meses** más cuando se trate de solicitudes especialmente complejas. En este caso el responsable deberá notificar, al interesado, esta ampliación dentro del primer mes.

- Si el responsable decide **no atender una solicitud**, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación e informará de la posibilidad de presentar una reclamación ante las autoridades de control, artículo 12.4 RGPD.

- En caso que la solicitud no contemple la información requerida, el responsable deberá solicitar la **subsanación** de la misma.

- Los interesados podrán ponerse en contacto con la **Delegada de Protección de Datos** de la UNED, en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.

- Corresponderá al responsable la **prueba** del cumplimiento del deber de respuesta, debiendo conservar la acreditación del cumplimiento del mencionado deber.

2.7.2. El derecho de acceso

Concepto y contenido del derecho

El artículo 15 del RGPD define el derecho de acceso como el derecho del interesado a solicitar y obtener del responsable del tratamiento, gratuitamente, información sobre el tratamiento de sus datos de carácter personal.

El afectado delimita con gran libertad el alcance del derecho de acceso, ya que puede optar a obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero o a la totalidad de sus datos sometidos a tratamiento.

El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, así como la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
El solicitante tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no, datos personales que le conciernen y, en caso de que se confirme el tratamiento, el acceso a los datos y la siguiente información:

- Los fines del tratamiento.
- Las categorías de datos personales de que se trate.
- Los destinatarios o las categorías de destinatarios a quienes han sido o serán comunicados los datos personales, en particular los destinatarios establecidos en terceros países o las organizaciones internacionales.
- El plazo previsto durante el cual se conservarán los datos personales, cuando esto no sea posible, los criterios utilizados para determinar este plazo.
- La existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de datos personales o la restricción del tratamiento de los datos personales relativos al interesado o a oponerse al tratamiento de dichos datos.
- El derecho a presentar una reclamación ante una autoridad de control.
- Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen.
- En el caso de las decisiones basadas en un tratamiento automatizado que comprenda la elaboración de perfiles, información sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento la importancia y las consecuencias previstas de dicho tratamiento
- Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías apropiadas.

El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable, basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

El derecho a obtener una copia no afectará negativamente a los derechos y libertades de los demás.

2.7.3. El derecho de rectificación

Concepto y contenido del derecho

El artículo 16 del RGPD define el derecho de rectificación como el derecho que tiene el interesado a rectificar sus datos cuando sean inexactos. Habida cuenta de los fines para los cuales hayan sido tratados los datos, el interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos, en particular por medio de la entrega de una declaración.

Conforme a lo dispuesto en el Considerando 39 del RGPD, "*el responsable del tratamiento debe establecer plazos para la revisión de los datos objeto de tratamiento y en su caso supresión. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.*"

2.7.4. Derecho de supresión

Concepto y contenido del derecho de supresión

El artículo 17 del RGPD define el derecho a la supresión como el derecho del interesado a solicitar la supresión de sus datos, sin perjuicio del deber de bloqueo.

El responsable del tratamiento tendrá la obligación de borrar los datos personales sin demora injustificada cuando concurra alguna de las circunstancias siguientes:

- Los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados.
- El interesado ha retirado el consentimiento en que se basa el tratamiento y no exista otro fundamento jurídico para el tratamiento de los datos.
- El interesado se oponga al tratamiento de datos personales y no prevalezca otro motivo legítimo para el tratamiento.
- Los datos han sido tratados ilícitamente.
- Los datos deban suprimirse para el cumplimiento de una obligación legal de la Unión o Estados miembros, a la que esté sujeto el responsable del tratamiento.
- Los datos han sido recogidos en relación con la oferta de servicios de la sociedad de la información y no prevalezcan otros motivos legítimos para el tratamiento.

Derecho al olvido

El Derecho al olvido no está considerado un derecho autónomo o diferenciado de los demás derechos, sino que es la consecuencia de la aplicación del derecho al borrado o supresión. Es una manifestación de los derechos de cancelación u oposición en el entorno on-line. Cuando el responsable del tratamiento haya hecho públicos los datos personales y esté obligado a suprimir dichos datos, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que traten los datos de que el interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

No es necesario que el interesado sufra un perjuicio para que ejerza el derecho al olvido.

Limitaciones en la supresión de datos.

El derecho a la supresión (u olvido) no será de aplicación, si el tratamiento de los datos personales es necesario:

- Para el ejercicio del derecho a la libertad de expresión e información.
- Para el cumplimiento de una obligación legal que requiera el tratamiento de datos personales impuesta por el Derecho de la Unión o de un Estado miembro a la que esté sujeto el responsable del tratamiento o para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento.
- Por motivos de interés público en el ámbito de la salud pública.
- Con fines de archivo en interés público o de investigación científica e histórica, propósitos o fines estadísticos, en la medida en que el derecho de supresión haga imposible o perjudique seriamente la consecución de los objetivos de los fines de archivo en el interés público, o de investigación científica e históricos o los fines estadísticos.
- Para el reconocimiento, ejercicio o defensa de demandas judiciales.

2.7.5. Derecho de oposición

Concepto y contenido del derecho

El artículo 21 del RGPD define el Derecho de oposición como el derecho del interesado a oponerse, en cualquier momento, por motivos relacionados con su situación particular, a que los datos personales que le conciernan sean objeto de un tratamiento.

Ante el ejercicio del derecho de oposición el responsable del tratamiento dejará de tratar los datos personales.

El derecho de oposición no se aplicará cuando el responsable del tratamiento acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Marketing directo

Cuando el tratamiento de datos personales tenga por objeto el marketing directo, el interesado tendrá derecho a oponerse en cualquier momento al tratamiento de los datos personales que le conciernan destinados a dicha comercialización, que incluye perfiles en la medida en que se relaciona con el marketing directo.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

Plazo

¿Cuándo se comunica que se han dejado de tratar los datos?

Como máximo en el momento de la primera comunicación con el interesado, informándole claramente de ello.

Forma comunicación

La comunicación se realizará de modo separado de cualquier otra información.

Tratamiento a efectos de investigación científica e histórica, o estadísticos

Cuando los datos personales se traten a efectos de investigación científica e histórica, o estadísticos, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de los datos personales que le conciernan, salvo que el tratamiento sea necesario para realizar una tarea efectuada por motivos de interés público.

Derecho de oposición a decisiones basadas únicamente en tratamiento automatizado

El artículo 22 del RGPD define el Derecho de oposición a decisiones basadas únicamente en tratamiento automatizado como el derecho del interesado a no ser objeto de una decisión que evalúe aspectos personales relativos a él fundada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que tenga efectos jurídicos que le conciernan o que le afecte de modo significativo.

Conforme al artículo 4.4. del RGPD se entiende por elaboración de perfiles, "*toda forma de tratamiento automatizado de datos personales destinado a evaluar determinados aspectos personales propios de una persona física o a analizar o predecir en particular su rendimiento profesional, su situación económica, su localización, su estado de salud, sus preferencias personales, su fiabilidad o su comportamiento, ubicación* o movimientos de dicha persona física*"*

Supuestos *(Considerando 71 del RGPD)*

Denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna.

Cualquier forma de tratamiento de los datos personales en el que se evalúen aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos en la medida en que produce efectos legales que conciernen al interesado o le afectan de modo significativo.

Excepciones

Se debe permitir la toma de decisiones sobre la base de tal tratamiento, incluida la elaboración de perfiles, cuando:

1. Es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
2. Está autorizada por el Derecho de la Unión o de un Estado miembro al que el responsable del tratamiento esté sujeto y que establezca igualmente medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado;
3. Se basa en el consentimiento explícito del interesado.

Medidas a adoptar

En los casos 1 y 3 anteriores, el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

Límites al tratamiento automatizado

Las decisiones sobre la base de tratamientos automatizados, no se podrán basar en las categorías especiales de datos personales, salvo que el interesado haya dado su consentimiento explícito o el tratamiento es necesario por motivos de para el cumplimiento de una misión de especial interés público, sobre la base del Derecho de la Unión o la legislación del Estado. Siempre que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado

Categorías especiales de datos personales: datos que revelen el origen étnico o racial las opiniones políticas, religiosas o creencias filosóficas, la orientación sexual o la identidad de género, la afiliación y las actividades sindical, así como el tratamiento de datos genéticos o biométricos o de datos relativos a la salud o vida sexual y orientación sexual.

2.7.6. Derecho de limitación del tratamiento

Concepto y contenido del derecho a la limitación del tratamiento

El artículo 18 RGPD define el Derecho a la limitación del tratamiento como el derecho del interesado a obtener del responsable del tratamiento la limitación del tratamiento de los datos personales cuando:

a) El interesado impugne la exactitud de los datos, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los mismos

b) El responsable del tratamiento ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; o

c) El interesado se ha opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable del tratamiento prevalecen sobre los del interesado.

Consentimiento tratamiento posterior

Cuando el tratamiento de datos personales haya quedado limitado dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o con miras a la protección de los derechos de otra persona física o jurídica o por motivos de interés público importante.

Plazo

Todo interesado que haya obtenido la restricción de tratamiento será informado por el responsable del tratamiento antes de que se levante dicha restricción.

Considerando 67

Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los

datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

2.7.7. Derecho a la portabilidad

Concepto y contenido del derecho

El artículo 20 del RGPD define el derecho a la portabilidad como el derecho del interesado a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado y de uso habitual y de lectura mecánica y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se hubieran facilitado los datos.

Supuestos para su ejercicio

Este derecho se podrá ejercitar en los siguientes casos:

a) El tratamiento esté basado en el consentimiento o en un contrato.

b) El tratamiento se efectúe por medios automatizados.

El ejercicio de este derecho se entenderá sin perjuicio del ejercicio del derecho a la supresión.

Supuestos en los que no se aplicará:

El derecho a la portabilidad de datos no se aplicará:

1. Al tratamiento necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento.
2. Cuando la revelación de los datos personales vulnere los derechos de propiedad intelectual respecto del tratamiento de dichos datos personales.

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 el RGPD. 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 de Conducta, 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 materia. 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. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Responsables y encargados deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD. Constarán por escrito, inclusive en formato electrónico.

La UNED, como Universidad pública y sujeto enumerado en el artículo 77.1. de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ha hecho público un inventario de sus actividades de tratamiento accesible por medios electrónicos, en el Portal Web UNED. El mismo estará a disposición de la autoridad de control que lo solicite.

2.9.1. Registro de actividades como Responsable

La UNED, como responsable del tratamiento, llevará un registro de actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro contiene toda la información indicada a continuación:

a) El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable y del delegado de protección de datos.
b) Los fines del tratamiento.
c) Una descripción de las categorías de interesados y de las categorías de datos personales.
d) Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
e) En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1 del RGPD, la documentación de garantías adecuadas.
f) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
g) Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

2.9.2. Registro de actividades como Encargado de Tratamiento

La UNED como encargada de tratamiento, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos.

b) Las categorías de tratamientos efectuados por cuenta de cada responsable.
c) En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1 del RGPD, la documentación de garantías adecuadas.
d) Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

2.10. MEDIDAS DE RESPONSABILIDAD PROACTIVA

2.10.1. Responsabilidad Proactiva

La UNED, en el tratamiento de los datos personales, analiza la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas. Asimismo, determina las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento Europeo de protección de datos. Las citadas se actualizarán cuando sea necesario.
Ejemplos de tales medidas son: la propia elaboración de este Código de Conducta; la información de la página Web del Portal UNED; los procedimientos y normativas elaborados en materia de seguridad; la implantación de la figura de la Delegada de protección de datos y de la Oficina adscrita a la misma; la formación impartida a los usuarios de la UNED; las comunicaciones y reuniones con los responsables de tratamiento…

2.10.2. Protección de datos desde el diseño y por defecto

El objetivo de la protección de datos desde el diseño es incluir los principios de protección de datos dentro de la UNED de manera tal que los mismos estén presentes a lo largo de toda la vida del tratamiento, es decir, **desde el momento en que se diseña**, se pone en práctica y finalmente se suprime o finaliza el tratamiento.

Con este principio y, de manera práctica, antes de acometer cualquier servicio que implique tratamiento de datos se deberá considerar este principio como un elemento necesario a incluir.

En relación con la protección de datos por defecto, el RGPD señala que deberán aplicarse medidas técnicas y organizativas apropiadas con la finalidad de que **sólo** sean objeto de tratamiento **los datos personales realmente necesarios** para cada uno de los fines específicos del tratamiento (principio de minimización). Dicha obligación abarcaría en la UNED:

- A la cantidad de datos recogidos
- A la extensión de su tratamiento.
- Al plazo de conservación.
- A la accesibilidad.

Esto es muy relevante, pues no sólo basta con diseñar un servicio nuevo realizando un enfoque garantista en materia de protección de datos, sino que, además, por defecto el servicio debe garantizar el máximo grado de privacidad posible.

2.10.3. Medidas de seguridad

Las medidas de seguridad tienen como finalidades principales garantizar la integridad de la información, permitir su recuperación en caso de incidentes y evitar los accesos no autorizados a las mismas. Por ello, el RGPD contempla medidas de seguridad que deben adaptarse a las características de los tratamientos, al tipo de datos tratados o a la tecnología disponible en cada momento.

Para cada uno de los tratamientos se realizará su respectivo análisis de riesgo o evaluación de impacto de privacidad para determinar las medidas de seguridad a aplicar.

En todo caso se tendrán en cuenta:

a) El cifrado de datos personales en el tratamiento de categorías especiales de datos.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) La coordinación de la gestión en materia de seguridad por el Comité de Seguridad de la Información. Para ello evalua y valora la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.

2.10.4. Notificación de violaciones de seguridad

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como “quiebras de seguridad”, de una forma muy amplia, que incluye todo incidente 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. Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.
Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

La notificación ha de incluir un contenido mínimo:

- La naturaleza de la violación
- Categorías de datos y de interesados afectados
- Medidas adoptadas por el responsable para solventar la quiebra
- Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados

Los responsables deben documentar todas las violaciones de seguridad.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos.

El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.

2.11. ROLES Y RESPONSABILIDADES

El Responsable de Seguridad de la UNED: Es la persona o personas a las que el responsable del tratamiento 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 tratamientos automatizados: El Coordinador de Sistemas de Tecnología de la Información.
Para tratamientos no automatizados: La Jefa de la Sección de Protección de Datos.

El Gestor de Tratamiento: Es la figura intermedia entre el Responsable del tratamiento 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 tratamiento 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
  - La Secretaria Técnica, como Responsable del Servicio
  - El Jefe de Área de Sistemas y Bases de Datos
  - El Coordinador de Sistemas de Tecnología de la Información
  - La Secretaria General
  - La Jefa de Departamento de Política Jurídica de Seguridad de la Información
  - El Responsable de Seguridad de la Información
  - 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: El nombramiento de esta figura, de nueva creación por el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, ha recaído en la Jefa del Departamento de Política Jurídica de Seguridad de la Información, 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 DE CONDUCTA

Se constituye una **Comisión de Control del Código de Conducta** 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
- La Secretaria Técnica
- El Asesor en materia de seguridad, actuando como Secretario
- La Delegada 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 de Conducta 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 de Conducta, 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 de Conducta.

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 el RGPD o en el presente Código de Conducta. 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 del RGPD.

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 de Conducta de la UNED.

Este derecho se ejercitará mediante la remisión del escrito a la Comisión de control del Código de Conducta, 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 Tratamiento 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 el RGPD atribuye a la Agencia Española de Protección de Datos.

2.14. INFRACCIONES Y SANCIONES

El régimen sancionador regulado en el presente Código de Conducta, se establece sin perjuicio de la potestad sancionadora que el RGPD atribuye a la Agencia Española de Protección de Datos, así como el Real Decreto Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos

Infracciones leves

1. El retraso injustificado de la Universidad en la contestación a las solicitudes de ejercicios de los derechos del interesado (acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad) 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 de Conducta, cuando no supongan infracciones del RGPD.

Infracciones Graves

1. Comisión de dos infracciones leves en el plazo de un año natural.

2. Incumplimiento de las obligaciones establecidas en el RGPD.

3. No realización de las auditorías previstas en el RGPD y en la normativa vigente.

4. Poner trabas en la ejecución de las auditorías y controles periódicos 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 SATISFACCIÓN

1. De forma complementaria a la difusión del Código de Conducta, 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 SUGERENCIAS, QUEJAS O RECLAMACIONES incluido, asimismo, en el ANEXO 8.1. del presente Código de Conducta.
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 de Conducta.(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 DEL INTERESADO

1.1. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS DE LA UNED

1.2. FLUJOGRAMA DEL EJERCICIO DE LOS DERECHOS

1.3. SOLICITUD DE EJERCICIO DE DERECHOS

2. CUMPLIMIENTO DEL DEBER DE INFORMACIÓN

2.1. CLÁUSULA INFORMATIVA

2.2. CLÁUSULA MATRÍCULA

2.3. CLÁUSULA CARTA DE PAGO MATRÍCULA

2.4. CLÁUSULA CEMAV. Grabaciones con compensación económica

2.5. CLÁUSULA CEMAV. Grabaciones

2.6. CLÁUSULA SEGURIDAD Y CONTROL DE ACCESOS AL EDIFICIO

2.7. CLÁUSULA PARA LOS EMPLEADOS

2.8. CLÁUSULA CONVENIOS (de los datos facilitados por el prestador de servicios)

2.9. CLÁUSULA CURRICULUM VITAE

2.10. CLÁUSULA DE CONSENTIMIENTO PARA CESIÓN / COMUNICACIÓN DE DATOS

2.11. CLÁUSULA CORREO ELECTRÓNICO

2.12. CLÁUSULA PRÁCTICAS FORMATIVAS-BECARIOS

2.13. CLÁUSULA VIDEO VIGILANCIA

2.14. TEXTO INFORMATIVO SOBRE LOS FICHEROS TEMPORALES

2.15. CLÁUSULA DE CONSENTIMIENTO TANSFERENCIAS INTERNACIONALES DE DATOS

2.16. AVISO LEGAL

2.17. POLÍTICA DE PRIVACIDAD

2.18. PERFIL DEL CONTRATANTE

3. FORMACIÓN

3.1. CURSOS IMPARTIDOS EN LA UNED SOBRE PROTECCION DE DATOS, NUEVAS TECNOLOGÍAS, SEGURIDAD DE LA INFORMACIÓN Y TRANSPARENCIA Y ASISTENCIA A SEMINARIOS Y JORNADAS DE PROTECCIÓN DE DATOS Y TRANSPARENCIA

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. NORMATIVA DE GESTIÓN DE INCIDENTES Y VIOLACIONES DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

4.7. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES Y VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES

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 A INSERTAR EN UN CONTRATO DE ENCARGADO DE TRATAMIENTO

5.2. CONTRATO DE ENCARGO DE TRATAMIENTO

5.3. COMPROMISO DE GUARDAR SECRETO PROFESIONAL Y PROHIBICIÓN DE ACCESO A DATOS

6. TRATAMIENTOS

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 TRATAMIENTO DE DATOS PERSONALES

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 TRATAMIENTOS 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. DIA DE PROTECCIÓN DE DATOS EN EUROPA

10.2. COMUNICADO SOBRE DESECHADO DE DOCUMENTOS EN PAPEL

10.3. CIRCULAR A LOS RESPONSABLES DE TRATAMIENTOS. NOVEDADES RGPD

10.4. COMUNICADO SOBRE LA UTILIZACIÓN DE BASES DE DATOS Y DERECHOS DE LOS ESTUDIANTES

10.5. COMUNICADO USO ALEATORIO DEL DNI

ANEXO 1.1.

Procedimiento interno para el ejercicio de los derechos en materia de protección de datos de la UNED

Departamento de Política Jurídica de Seguridad de la Información

ÍNDICE

INTRODUCCIÓN 2
1. OBJETO 2
2. NORMATIVA 2
3. FUNCIONES Y RESPONSABILIDADES EN LA UNED 3
4. NATURALEZA DE LOS DERECHOS 3
5. NOTAS COMUNES AL EJERCICIO DE DERECHOS 6
6. MEDIOS DE PRESENTACIÓN DE LAS SOLICITUDES 7
7. ACTUACIONES ANTE LA SOLICITUD DEL EJERCICIO DE DERECHOS 7

INTRODUCCIÓN

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD), dedica su Capítulo III a regular los Derechos de los interesados, introduciendo novedades que mejoran la capacidad de decisión y control de los ciudadanos sobre sus propios datos personales; asimismo, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, dedica su Título III a los derechos de las personas.

A los tradicionales derechos existentes en la normativa anterior vigente de protección de datos, los derechos ARCO, acceso, rectificación, cancelación y oposición, el RGPD añade nuevos derechos como son el derecho a la portabilidad de los datos, el derecho a la limitación en el tratamiento y el derecho de supresión, o derecho al olvido, que se ha venido considerando incluido dentro del derecho de cancelación y oposición.

El derecho a la protección de datos de carácter personal como derecho fundamental, en España, se ha ido construyendo, por el Tribunal Constitucional a través de su sentencias, considerándose un derecho derivado del artículo 18.4 de la Constitución Española, el cual dispone: *"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"*.

En este sentido la **UNED:**

INFORMA sobre el derecho fundamental a la protección de datos.

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 normativa vigente.

GARANTIZA el derecho a la protección de datos cumpliendo con lo establecido en la legislación vigente.

1. OBJETO

El objeto de este documento es establecer el procedimiento para la tramitación de las solicitudes del ejercicio de los derechos en materia de protección de datos, sobre los datos de carácter personal que figuren en poder de la Universidad.

2. NORMATIVA

- 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
- LEY ORGÁNICA 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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.

- **FUNCIONES Y RESPONSABILIDADES EN LA UNED**

Responsable de Tratamiento

- Tramitar y resolver las solicitudes enviadas por los interesados, 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 tratamiento

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

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 solicitados por el titular de los datos.

Delegada de Protección de Datos

- Actuar como punto de contacto con los interesados en lo relativo al tratamiento de sus datos personales y al ejercicio de sus derechos.

3. NATURALEZA DE LOS DERECHOS

Derecho de Acceso

El derecho de acceso viene regulado en al art. 15 del RGPD y se recoge en los considerandos 63 y 64, como un derecho del interesado a obtener, del responsable del tratamiento, confirmación de si se están tratando o no datos personales que le conciernen. Así, de la regulación del Derecho de Acceso contenida en el RGPD se desprende que, en caso de que se estén tratando sus datos personales, el interesado puede acceder a los mismos y a la siguiente información:

- Finalidad del tratamiento.
- Categoría de los datos personales que se tratan.
- Destinatarios o categorías de destinatarios a los que se les comunicará estos datos.
- Plazo previsto de conservación o, si no es posible, los criterios para su determinación.

- La existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de datos personales o la restricción del tratamiento de los datos personales relativos al interesado o a oponerse al tratamiento de dichos datos.
- Existencia del derecho a presentar una reclamación ante la autoridad de control.
- Cuando los datos personales no se hayan obtenido del interesado, se le facilitará cualquier información disponible sobre su origen.
- En el caso de las decisiones basadas en un tratamiento automatizado que comprenda la elaboración de perfiles, información sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento.
- Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías apropiadas.

Derecho de Rectificación

El derecho de rectificación, viene regulado en el Artículo 16 del RGPD, como el derecho que tiene el interesado a solicitar del responsable del tratamiento la rectificación de sus datos cuando sean inexactos. Ante esta solicitud el responsable deberá satisfacer este derecho sin dilación indebida. Derecho que en idénticos términos recoge el Considerando (65).

Teniendo en cuenta los fines para los cuales hayan sido tratados los datos, el interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos, en particular por medio de la entrega de una declaración.

Derecho de Supresión

El derecho a la supresión, derecho al olvido, regulado en el artículo 17 del RGPD, es la denominación que da el Reglamento al tradicional derecho de cancelación, que regula la LOPD y su Reglamento de desarrollo.

En base al mismo el interesado tendrá derecho a obtener, sin dilación indebida del responsable del tratamiento, la supresión de los datos personales que le conciernan, cuando concurra alguna de las circunstancias siguientes:

- Cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- Cuando el interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico.
- Cuando el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.
- Cuando los datos personales hayan sido tratados ilícitamente.
- Cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- Cuando los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información dirigidos a menores.

El responsable del tratamiento estará obligado a suprimir sin dilación indebida los datos personales, ante la solicitud de un derecho de supresión en la que se den las circunstancias que recoge el RGPD.

Derecho de oposición

El derecho de oposición viene regulado en el artículo 21 del RGPD y en los Considerandos (69) y (70). Podemos decir que es el derecho del interesado a oponerse, en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento.

Ante el ejercicio del derecho de oposición el responsable del tratamiento dejará de tratar los datos personales. Sin embargo no es este un derecho absoluto del interesado, por lo que procederá, en algunos supuestos realizar una ponderación con el fin de considerar si prevalece o no el derecho del interesado.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines. Así pues en estos casos no procederá realizar ponderación alguna.

Derecho a la Portabilidad

El derecho a la portabilidad es uno de los nuevos derechos que regula el RGPD, en su artículo 20 y el Considerando (68).

Señala el artículo 20.1 RGPD: *"El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado".*

De la lectura del artículo podemos señalar que el derecho a la portabilidad es el derecho que permite al interesado recibir los datos que ha proporcionado al responsable y le faculta a transmitirlos, a otro responsable del tratamiento, sin impedimentos.

Derecho a la Limitación

El artículo 4 del RGPD, en sus definiciones incluye la de limitación del tratamiento: "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro". Se trata de una medida cautelar que reduce el tratamiento de los datos personales a la conservación.

Los supuestos en los que el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos están tasados por el artículo 18 del RGPD y son:

- Cuando el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
- Cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- Cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- Cuando el interesado se haya opuesto al tratamiento ejercitando su derecho de oposición, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

4. NOTAS COMUNES AL EJERCICIO DE DERECHOS

El RGPD no sólo modifica el catálogo de derechos, sino que además introduce novedades en el procedimiento para su ejercicio.

- Se ha de aplicar en todo momento el **Principio de Transparencia**. Toda la información que se dirija al interesado ha de ser concisa, de fácil acceso y a través de un lenguaje claro y sencillo.
- Los responsables deben **facilitar a los interesados el ejercicio de sus derechos**. Este mandado contenido en el artículo 12.2 RGPD supone que los procedimientos y las formas que se faciliten a los interesados, para el ejercicio de sus derechos, deben ser visibles, accesibles y sencillos.
- A diferencia de la actual regulación, en el RGPD **se establece como una obligación** expresa de los responsables hacer efectivos los derechos del interesado.
- Se requiere que los Responsables posibiliten la **presentación de solicitudes por medios electrónicos**, especialmente cuando el tratamiento se realiza por estos medios.
- El ejercicio de los derechos será **gratuito** para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas.
- Se trata de **derechos independientes**, es decir, que el ejercicio de ninguno de ellos es requisito previo para el ejercicio del otro.
- El responsable que trate una **gran cantidad de información** sobre un interesado podrá pedir a éste que especifique la información a que se refiere su solicitud de acceso.
- El responsable podrá contar con la **colaboración de los encargados** para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.
- Ante la solicitud de ejercicio de derechos el responsable deberá informar al interesado sobre las actuaciones derivadas de su petición en el **plazo de un mes,** artículo 12.3 RGPD. Este plazo podrá **extenderse dos meses** más cuando se trate de solicitudes especialmente complejas. En este caso el responsable deberá notificar, al interesado, esta ampliación dentro del primer mes.

  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.*

- Si el responsable decide **no atender una solicitud**, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación e informará de la posibilidad de presentar una reclamación ante las autoridades de control, artículo 12.4 RGPD.

- En caso que la solicitud no contemple la información requerida, el responsable deberá solicitar la **subsanación** de la misma.
- La **prueba** del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado, recaerá sobre el responsable.
- Los interesados podrán ponerse en contacto con la **Delegada de Protección de Datos** de la UNED, en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.

5. MEDIOS DE PRESENTACIÓN DE LAS SOLICITUDES

PRESENCIALMENTE:
Cumplimentando el formulario de solicitud 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 en materia de protección de datos.

6. ACTUACIONES ANTE LA SOLICITUD DEL EJERCICIO DE LOS DERECHOS

El ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al Responsable del Tratamiento, 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.

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 6 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.
   - Actividad de tratamiento afectada y responsable de su tramitación.
   - Fecha de comunicación al Responsable del Tratamiento.
   - Fecha máxima de contestación del Responsable del Tratamiento.
   - Fecha de notificación al interesado.

5. En el plazo máximo de 48 horas, el Departamento de Política Jurídica de Seguridad de la Información remitirá la solicitud, la documentación pertinente y la información relativa a los plazos límites de respuesta, al Responsable del Tratamiento correspondiente.

6. El Responsable del Tratamiento, 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 a la Unidad 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 en materia de protección de datos, de la Sede electrónica.

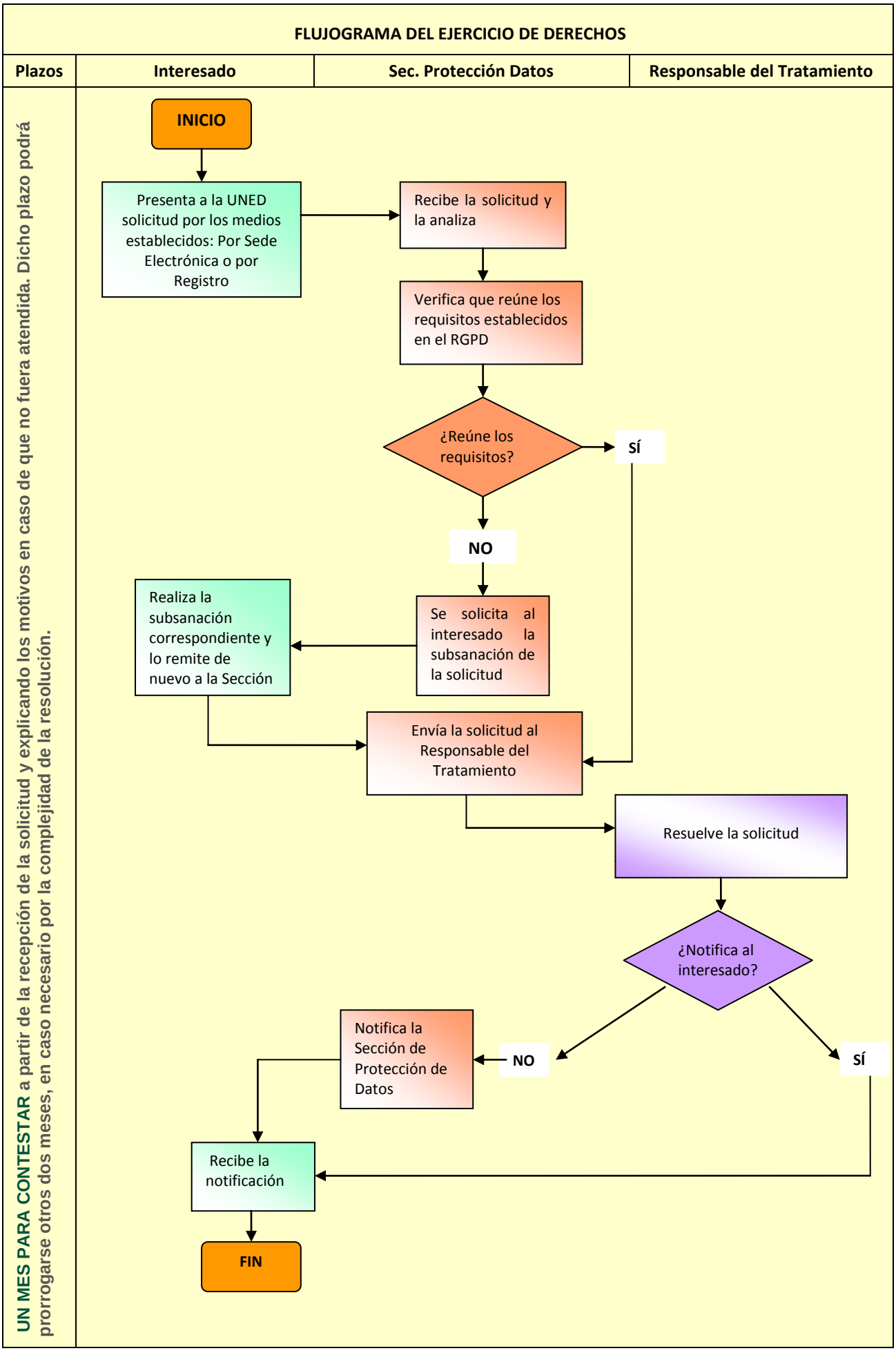
2. El acceso a la Sede requiere el uso de un certificado digital para las firmas y comparecencias, reconocido por cualquiera de las entidades oficiales de certificación nacionales.

3. Las solicitudes se recibirán en el 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 7.2.4. 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, la Unidad remitirá la solicitud, la documentación pertinente y la información relativa a los plazos límites de respuesta, al Responsable del Tratamiento correspondiente.

5. El Responsable del Tratamiento, encargado del trámite, resolverá la solicitud dentro del plazo establecido y elaborará la notificación al interesado, remitiéndola a la Unidad tramitadora, que a través de la Sede, la enviará al interesado.


FLUJOGRAMA DEL EJERCICIO DE DERECHOS
Plazos
Interesado
Sec. Protección Datos
Responsable del Tratamiento
UN MES PARA CONTESTAR a partir de la recepción de la solicitud y explicando los motivos en caso de que no fuera atendida. Dicho plazo podrá prorrogarse otros dos meses, en caso necesario por la complejidad de la resolución.
INICIO
Presenta a la UNED solicitud por los medios establecidos: Por Sede Electrónica o por Registro
Recibe la solicitud y la analiza
Verifica que reúne los requisitos establecidos en el RGPD
¿Reúne los requisitos?
SÍ
NO
Se solicita al interesado la subsanación de la solicitud
Realiza la subsanación correspondiente y lo remite de nuevo a la Sección
Envía la solicitud al Responsable del Tratamiento
Resuelve la solicitud
¿Notifica al interesado?
NO
SÍ
Notifica la Sección de Protección de Datos
Recibe la notificación
FIN

ANEXO 1.3.

EJERCICIO DE DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS

DATOS DEL RESPONSABLE DEL TRATAMIENTO

Código de la unidad tramitadora: U2800039
Departamento de Política Jurídica de Seguridad de la Información
Nombre / razón social: Universidad Nacional de Educación a Distancia
Dirección ante la que se ejercita el derecho:
Calle Bravo Murillo nº 38. 28015-MADRID
CIF: Q2818016D

DERECHO A EJERCITAR

- ☐ **Acceso**
- ☐ **Rectificación**
- ☐ **Supresión**
- ☐ **Limitación del tratamiento**
- ☐ **Portabilidad de los datos**
- ☐ **Oposición**

Justificar la petición:

DATOS DEL INTERESADO O REPRESENTANTE LEGAL [1]

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 señalado anteriormente, de conformidad con lo previsto en los artículos 12 al 22 del Reglamento General Europeo de 27 de abril de 2016 y en consecuencia,

SOLICITA,

Que se le facilite, gratuitamente, el derecho anteriormente expuesto en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes.

En a de de 20

Firmado,

[1] 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

Es necesario aportar **fotocopia del DNI** o documento equivalente que acredite la identidad y sea considerado válido en derecho, para que el responsable del tratamiento 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.

Denegación:

- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante La Agencia Española de Protección de Datos (www.agpd.es).

- Los interesados podrán ponerse en contacto con la Delegada de Protección de Datos de la Universidad, en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos, a través del e-mail: dpd@adm.uned.es

ANEXO 2.1.

CLÁUSULA INFORMATIVA

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

La finalidad del tratamiento de los datos es _____

Las bases legitimadoras por las que se tratan sus datos son: (el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de una obligación legal aplicable al responsable del tratamiento)_____

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.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad

ANEXO 2.2.

CLÁUSULA MATRÍCULA

INFORMACIÓN RELATIVA A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED).

La finalidad del tratamiento 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.

La base jurídica por la cual se tratan sus datos es la ejecución del servicio público de educación que presta la UNED.

Los datos podrán ser cedidos o comunicados, cuando legalmente proceda, a los Centros Asociados a la UNED y a las Administraciones Públicas competentes en materia educativa y en el caso de domiciliar el pago de los precios públicos, se comunicarán a las entidades bancarias, los datos estrictamente necesarios para la gestión del pago, así como a requerimiento de la Agencia Tributaria, Juzgados o Tribunales.

He sido informado y acepto… ☐

Asimismo, le informamos que sus datos podrán ser utilizados a fin de mantenerle informado, por cualquier medio de contacto (incluidas las comunicaciones electrónicas), 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. ☐

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad

ANEXO 2.3.

CLÁUSULA CARTA DE PAGO DE LA MATRÍCULA

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

La finalidad del tratamiento 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.

Las bases legitimadoras por las que se tratan sus datos son: (el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de una obligación legal aplicable al responsable del tratamiento)_____

Los datos podrán ser cedidos o comunicados, cuando legalmente proceda, a los Centros Asociados a la UNED y a las Administraciones Públicas competentes en materia educativa y en el caso de domiciliar el pago de los precios públicos, se comunicarán a las entidades bancarias, los datos estrictamente necesarios para la gestión del pago, así como a requerimiento de la Agencia Tributaria, Juzgados o Tribunales.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento, ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

ANEXO 2.4.

AUTORIZACIÓN GRABACIONES
CON COMPENSACIÓN ECONÓMICA- CEMAV

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos facilitados a través del presente impreso serán tratados, en calidad de **Responsable del tratamiento**, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED)

La **finalidad** del tratamiento es gestionar su participación en programas de Radio, Televisión u otros medios, producidos por el CEMAV, así como las autorizaciones y liquidaciones de las compensaciones económicas que pudieran acordarse por su intervención en calidad de conferenciante de la UNED. Las bases legitimadoras por las que se tratan sus datos son:(el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de una obligación legal aplicable al responsable del tratamiento)_____

Los datos podrán ser 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 en la Ley, y a las entidades bancarias, los datos estrictamente necesarios para la gestión del pago, así como a requerimiento de la Agencia Tributaria, Juzgados o Tribunales.

Asimismo, debe tener en cuenta que la publicación de grabaciones de imagen y/o voz en redes sociales u otras plataformas de Internet, podrá comportar una transferencia internacional de datos ya que los servidores de dichas plataformas pueden radicar en EEUU o/y otros países fuera de la UE , que se entiende no proporcionan un nivel de protección equiparable, por lo que, para el caso de que dicha transferencia no pueda realizarse en base a una decisión de adecuación o a través del establecimiento de las garantías adecuadas, se solicita también autorización para realizar dicha transferencia. Asimismo, la publicación de imágenes en dichas plataformas externas supone la aceptación de sus políticas de privacidad.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40)de la UNED.

El presente consentimiento comprende, asimismo, la digitalización y el procesamiento de las grabaciones de imagen y sonido. Por tanto, autoriza la cesión con carácter gratuito y hasta el momento en que los derechos que legalmente le correspondan se extingan o revoque su autorización, de los derechos necesarios en materia de propiedad intelectual, en cuanto a la elaboración, reproducción, distribución, exposición o retransmisión pública de las grabaciones de imagen y sonido.

Para más información visite nuestra Política de Privacidad.

Nombre y apellidos: _____DNI _____-Firmado _____

En Madrid a ___de ___ de 20__

ANEXO 2.5.

MODELO CLÁUSULA CEMAV –AUTORIZACIÓN DE LAS GRABACIONES

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos personales facilitados a través del presente impreso serán tratados, en calidad de **Responsable del tratamiento**, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED).

La finalidad es la de gestionar la participación en los programas de Radio, Televisión u otros medios producidos por el CEMAV.

Las bases legitimadoras por las que se tratan sus datos son: (el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de una obligación legal aplicable al responsable del tratamiento) _____

Asimismo, le informamos 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.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

ANEXO 2.6.

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 trascripción 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

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

La finalidad es la seguridad y control de acceso al edificio de la Institución.

La base jurídica por la cual se tratan sus datos es el interés público de control de acceso y vigilancia de las instalaciones.

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.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

ANEXO 2.7.

CLÁUSULA INFORMATIVA SOBRE PROTECCIÓN DE DATOS PERSONALES PARA LOS EMPLEADOS

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

Las bases legitimadoras por las que se tratan sus datos son: (el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de una obligación legal aplicable al responsable del tratamiento) _____

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 funcionarial).

- **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.

Cuando legalmente proceda, los datos podrán ser cedidos o comunicados a:

- 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.
- A las entidades bancarias exclusivamente para el pago de salarios.
- 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.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

Fecha:

Firmado:
NOMBRE Y APELLIDOS DEL EMPLEADO

ANEXO 2.8.

CLÁUSULA CONVENIOS

DE LOS DATOS FACILITADOS POR EL PRESTADOR DE SERVICIOS

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

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

La base jurídica por la cual se tratan sus datos es la ejecución del contrato en el que el interesado es parte.

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.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

ANEXO 2.9.

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

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

La 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.

Las bases legitimadoras por las que se tratan sus datos son: (el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de una obligación legal aplicable al responsable del tratamiento) _____

Los datos personales no serán cedidos o comunicados a terceros, salvo obligación legal.

El plazo de conservación será de … años.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

ANEXO 2.10.

CLÁUSULA DE CONSENTIMIENTO PARA CESIÓN / COMUNICACIÓN DE DATOS PERSONALES

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

La finalidad del tratamiento es_____

Las bases legitimadoras por las que se tratan sus datos son:(el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de una obligación legal aplicable al responsable del tratamiento)_____

Los datos podrán ser cedidos o comunicados, cuando legalmente proceda, a [identificar los destinatarios de los datos]

La cesión de sus datos personales a [indicar destinatarios de los datos localizados en países fuera de la UE] comporta una transferencia internacional de datos que se entiende no proporciona un nivel de protección equiparable, por lo que, para el caso de que dicha transferencia no pueda realizarse en base a una decisión de adecuación o a través del establecimiento de las garantías adecuadas, se solicita también autorización para realizar dicha transferencia.

Podrá ejercitar los derechos de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

☐ Autorizo la cesión/comunicación de mis datos a las entidades indicadas

☐ Autorizo la transferencia internacional de datos a las entidades que se encuentren fuera de la UE

Fdo.:

ANEXO 2.11.

CLÁUSULA DEL CORREO ELECTRÓNICO ADAPTADA AL RGPD

AVISO LEGAL. Este mensaje puede contener información reservada y confidencial. 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, serán tratados en calidad de responsable de tratamiento por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED) c/ Bravo Murillo, 38, 28015-MADRID-, con la finalidad de mantener el contacto con usted. Las bases legitimadoras por las que se tratan sus datos son: el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

En cualquier momento podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación al tratamiento o portabilidad de los datos, ante la UNED, Departamento de Política Jurídica de Seguridad de la Información, o a través de la Sede electrónica de la Universidad.

Para más información visite nuestra *Política de Privacidad*

ANEXO 2.12.

CLÁUSULA PRÁCTICAS FORMATIVAS-BECARIOS

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos aportados en este documento serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

La finalidad del tratamiento es la gestión y tramitación de las solicitudes de personas interesadas en la realización de prácticas en calidad de becario en formación.

La base legitimadora por las que se tratan sus datos es la ejecución de un contrato en el que el interesado es parte.

Los datos personales que contengan información de carácter fiscal o laboral serán cedidos o comunicados 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, 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.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

Firmado:

NOMBRE Y APELLIDOS

ANEXO 2.13.

DEBER DE INFORMACIÓN EN RELACIÓN CON LA VIDEOVIGILANCIA

Partiendo de la premisa de que las imágenes son un dato de carácter personal, de conformidad con lo establecido en La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, sobre los tratamientos con fines de Videovigilancia, 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 los artículo 12 del Reglamento UE 2016/679 General de Protección de Datos Personales (RGPD). A tal fin deberán:

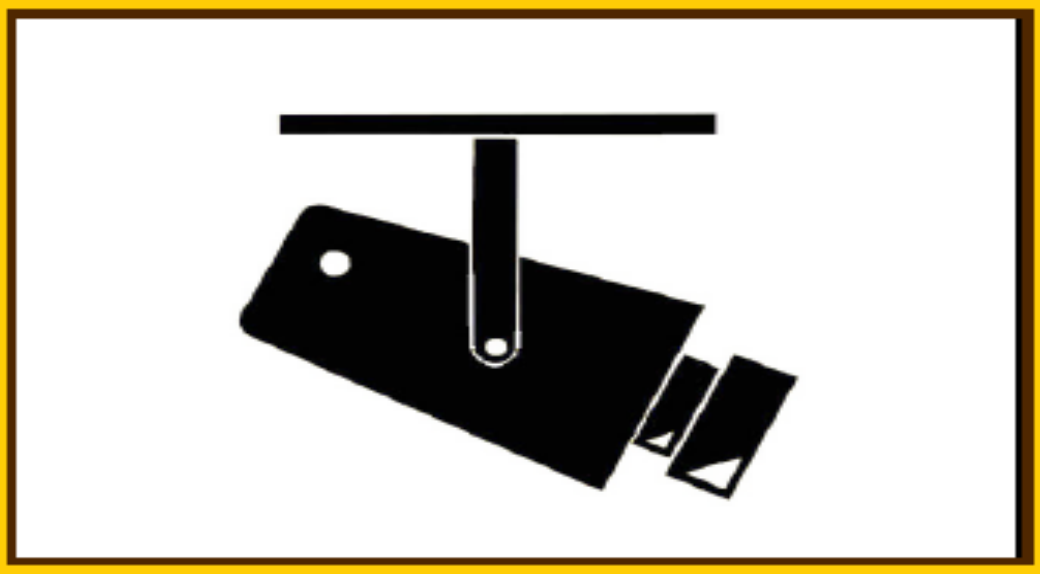
a) Colocar, en las zonas video vigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados.
b) Tener a disposición de los interesados impresos en los que se detalle la información prevista en los artículos 12 a 15 del RGPD. El contenido 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 AGPD:

- 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.

ZONA VIDEOVIGILADA



REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016, (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS)

PUEDE EJERCITAR LOS DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, Y OTROS DERECHOS ANTE LA UNED.
C/ Bravo Murillo, 38 28015-MADRID
www.uned.es/dpj

MÁS INFORMACIÓN
SOLICITAR EN MOSTRADOR *DE ENTRADA*

CLÁUSULA INFORMATIVA DE VIDEOVIGILANCIA

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, se informa de:

1. Que el responsable del tratamiento de los datos personales es la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED).
2. La finalidad del tratamiento es de preservar la seguridad, personal y material, en las diferentes sedes e instalaciones de la UNED, a través de un sistema de videovigilancia.
3. La base jurídica del tratamiento reside en los intereses públicos del responsable de garantizar la seguridad de las personas, bienes e instalaciones
4. 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.

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

Para más información visite nuestra Política de Privacidad.

ANEXO 2.14

COPIAS DE TRABAJO DE DOCUMENTOS

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

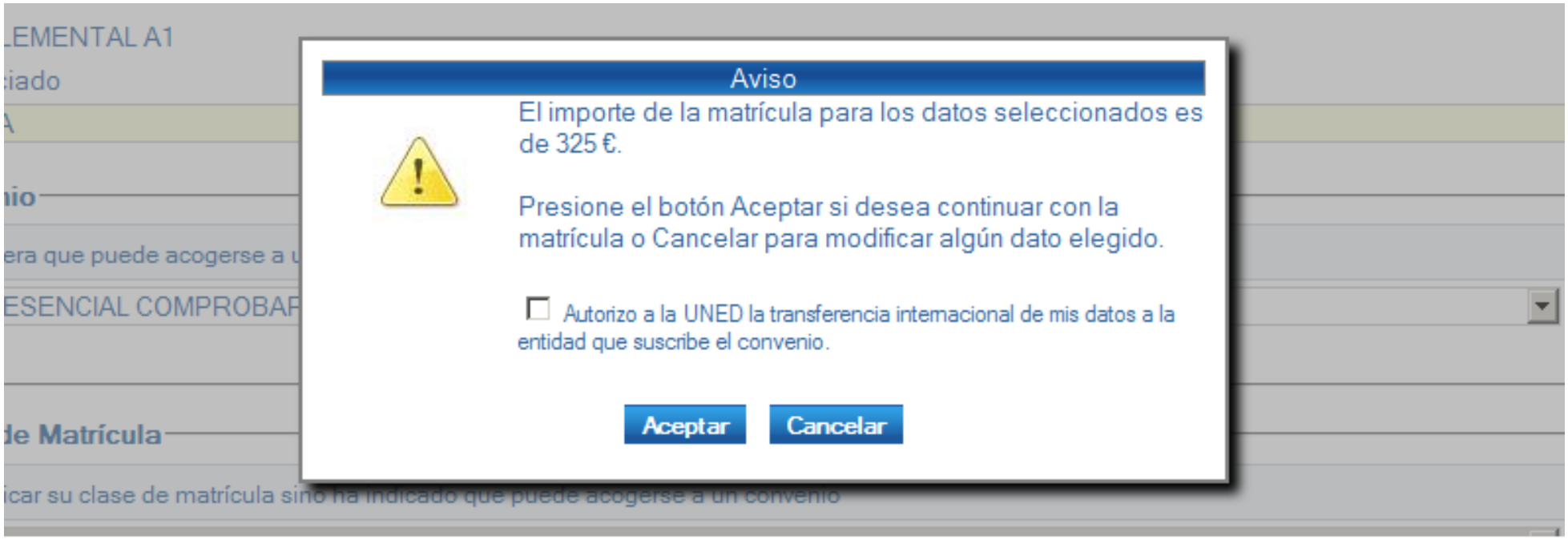
Es importante recordar que la utilización de los mismos requiere el cumplimiento de los Principios relativos al tratamiento de datos personales del Reglamento (UE) 2016/679, de 27 de abril, de Protección de Datos (RGPD). En este sentido el art.5.1. señala que: ***"los datos personales serán exactos y si fuera necesario, actualizados"; "serán mantenidos durante no más tiempo del necesario para los fines del tratamiento"***

De no cumplir con estos principios, estaríamos ante una infracción muy grave según el art.72 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por ello, **toda copia de trabajo será borrada o destruida una vez que haya dejado de ser necesaria** 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 2.15.

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



ANEXO 2.16.

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). La UNED es el titular del portal.
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 NIF 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. O mediante Email a la siguiente dirección: **infouned@adm.uned.es**

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.

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.

En todo caso, la persona afectada por una publicación en el sitio Web de su imagen, podrá revocar el consentimiento que hubiese prestado, y ejercitar los derechos de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante, la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y formularios: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj)
o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED

IV. CONDICIONES Y TÉRMINOS DE USO DEL SITIO 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.

   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 sean contrarias 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.
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.

7. La UNED no será responsable de los daños y perjuicios que, en su caso, se puedan causar al usuario con motivo del acceso y uso de su cuenta por parte de terceros sin autorización.

VII MODIFICACIONES:

La UNED se reserva el derecho de efectuar sin previo aviso las modificaciones que considere oportunas en su portal, pudiendo cambiar, suprimir o añadir tanto los contenidos y servicios que se presten a través de la misma como la forma en la que éstos aparezcan presentados o localizados en su portal.

VIII DERECHO DE EXCLUSIÓN:

La UNED se reserva el derecho a denegar o retirar el acceso a portal sin necesidad de preaviso, a instancia propia o de un tercero, a aquellos usuarios que incumplan el presente Aviso Legal.

La UNED se reserva el derecho de retirar todos aquellos comentarios y aportaciones realizados por los usuarios que vulneren el respeto a la dignidad de la persona, que sean discriminatorios, xenófobos, racistas, pornográficos, que atenten contra la juventud o la infancia, el orden o la seguridad pública o que, a su juicio, no resultaran adecuados para su publicación.

IX GENERALIDADES y MISCELÁNEA

La UNED perseguirá el incumplimiento de las presentes condiciones así como cualquier utilización indebida de su portal ejerciendo todas las acciones civiles y penales que le puedan corresponder en derecho. La UNED se reserva el derecho de ejercitar todas las acciones posibles conforme a la legislación española.

La UNED podrá poner en conocimiento y colaborar oportunamente con las autoridades policiales y judiciales competentes si detectase cualquier infracción de la legislación vigente o si tuviera sospecha de delito o falta penal.

En cumplimiento de la legislación española, la UNED se compromete a realizar esta tarea con la máxima diligencia posible de acuerdo con sus capacidades técnicas.

X. 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 2.17.

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 espacio **www.uned.es** en lo referente al 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. RESPONSABLE DEL TRATAMIENTO

Nombre del Responsable: UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

Dirección: Calle Bravo Murillo 38, Madrid, 28015

Correo electrónico: infouned@adm.uned.es

Datos de contacto del Delegado de Protección de Datos: dpd@adm.uned.es

III. FINALIDAD DEL TRATAMIENTO

La UNED tratará sus datos personales con las finalidades indicadas a continuación, dependiendo de la situación en que los datos de carácter personal sean recogidos.

Se informará en cada caso de la finalidad concreta del tratamiento:

- 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.

- Seguridad y control de acceso al edificio de la Institución

- Recogida y tratamiento de la información para la gestión del contrato suscrito o de los servicios solicitados.

- 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.

- Gestión y tramitación de las solicitudes de personas interesadas en la realización de prácticas en calidad de becario en formación.

- Gestionar su participación en programas de Radio, Televisión u otros medios, producidos por el CEMAV, así como las autorizaciones y liquidaciones de las compensaciones económicas que pudieran acordarse por su intervención en calidad de conferenciante de la UNED.

IV BASES DE LEGITIMACIÓN

La UNED tratará sus datos personales de acuerdo con la base de legitimación de la que se informará debidamente al interesado en cada situación:

- El consentimiento del interesado.
- La ejecución de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- La ejecución de un contrato en que el interesado es parte o para la aplicación a petición de este de las medidas precontractuales.
- En los tratamientos de control de acceso o Videovigilancia, la base legal será el interés legítimo perseguido por la UNED.

V. PLAZOS DE CONSERVACIÓN DE LOS DATOS

Los datos serán conservados durante el tiempo mínimo necesario y en cualquier caso durante los plazos legalmente previstos.

La información tratada en base a la ejecución de un contrato, u otro tipo de relación de servicios será conservada hasta la finalización de la relación contractual o de la prestación de servicios.

Las imágenes grabadas para cumplir con la finalidad de seguridad se conservarán por un máximo de un mes.

Se podrá proceder al bloqueo y conservación de las imágenes para ponerlas a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

Los datos de los solicitantes de empleo o prácticas formativas serán conservados durante los plazos fijados en la convocatoria.

El interesado tiene derecho a revocar su consentimiento en cualquier momento y a ejercer los derechos reconocidos en el Reglamento General Europeo de Protección de Datos (ver apartado VII)

VI. 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.

Los datos podrán ser cedidos, cuando legalmente proceda, a:

- Los Centros Asociados a la UNED.
- Las Administraciones Públicas competentes en materia educativa.
- Las entidades bancarias, a efectos de la gestión de pagos.
- En el caso de que el interesado participe en algún programa de Radio, Televisión u otros medios, a los titulares de los medios en los que el interesado participe.
- A la Agencia Tributaria, la Seguridad Social o los Juzgados y Tribunales a requerimiento de estos órganos.

VII DERECHOS DE LOS USUARIOS

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

El interesado tiene derecho a retirar su consentimiento para el tratamiento de los datos en cualquier momento

El interesado tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, en caso de que considere que no se ha atendido correctamente el ejercicio de sus derechos. Para ello puede utilizar los recursos situados en la página web de la AEPD.

VIII. SEGURIDAD DE LOS DATOS Y UTILIZACIÓN DE COOKIES

La UNED aplica las medidas de seguridad técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que puede suponer el tratamiento.

La UNED utiliza *cookies* cuando el usuario navega por su página Web, que son activadas desde el servidor **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. Se utilizarán 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*.

En concreto este sitio web maneja las siguientes cookies de terceros:

Google Tag Manager y Google Analytics. Puede ampliar información sobre el uso de las cookies en la Política de Privacidad de Google: http://www.google.com/intl/en/policies/privacy/

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

ANEXO 2.18.

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".*

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

De conformidad con lo establecido en la Normativa vigente de Protección de Datos Personales, le informamos que los datos personales facilitados, como persona física, o en el caso de representantes de una persona jurídica, serán tratados, en calidad de Responsable del tratamiento, por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA.

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.

Las bases legitimadoras por las que se tratan sus datos son: la ejecución de un contrato en el que el interesado es parte o el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

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.

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

Podrá ejercitar los **derechos** de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de los datos u Oposición al tratamiento ante la UNED, C/ Bravo Murillo 38, Sección de Protección de Datos, 28015 de Madrid, o en cualquiera de las oficinas que podrá encontrar aquí, junto con información adicional y el formulario: Departamento de Política Jurídica de Seguridad de la Información, (www.uned.es/dpj) o a través de la Sede electrónica (https://sede.uned.es/procedimientos/portada/idp/40) de la UNED.

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. Las responsabilidades del Encargado del Tratamiento se regularán conforme al artículo 28 del Reglamento UE 2016/679 General de Protección de Datos.

En este sentido, los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Disposición Adicional Vigésima quinta de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

ANEXO 3.1.

CURSOS IMPARTIDOS EN LA UNED SOBRE PROTECCIÓN DE DATOS Y EL ESQUEMA NACIONAL DE SEGURIDAD (ENS)

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. Se ha impartido una conferencia sobre "los problemas derivados de las nuevas tecnologías y los foros académicos" en la Universidad de Murcia en noviembre de 2011 dentro de las Jornadas universitarias de los Servicios de Inspección.

5. Ha participado como ponente en el II Master de Calidad en la Gestión de Centros Universitarios, organizado por el Centro Asociado de Tudela (curso 2011-2012). La materia impartida fue la Protección de datos y su aplicación en los Centros Asociados de la UNED.

6. 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.

7. Curso *Protección de Datos y nuevas tecnologías* del 23 de octubre al 21 de noviembre de 2014, de 25 horas. En la modalidad presencial y on line, 6 horas presenciales y 19 horas on line.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. Curso Protección de Datos y Nuevas Tecnologías los días 22, 24 y 26 de mayo de 2017, de 9 horas de duración en la modalidad presencial.

14. Curso Protección de Datos y Nuevas Tecnologías los días 14, 16 y 21 de noviembre de 2017, de 9 horas de duración en la modalidad presencial.

15. Curso Seguridad y Transparencia en la Gestión de la Información los días 5, 7 y 9 de junio de 2017, de 9 horas de duración en la modalidad presencial.

16. Curso Seguridad y Transparencia en la Gestión de la Información los días 12, 14 y 16 de junio de 2017, de 9 horas de duración en la modalidad presencial.

17. Curso Seguridad y Transparencia en la Gestión de la Información los días 20, 22 y 27 de junio de 2017, de 9 horas de duración en la modalidad presencial.

18. Curso Seguridad y Transparencia en la Gestión de la Información los días 23, 28 y 30 de noviembre de 2017, de 9 horas de duración en la modalidad presencial.

19. Curso sobre la ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y Buen Gobierno los días 23, 26 y 28 de noviembre de 2018, de 9 horas de duración en la modalidad presencial.

20. Curso: "Legislación de Protección de Datos" realizado en el Centro Asociado de Madrid el 21 de junio de 2018, de 5 horas de duración en la modalidad presencial.

21. Curso: "Transparencia" realizado en el Centro Asociado de Madrid el 29 de junio de 2018, de 5 horas de duración en la modalidad presencial.

22. Curso: " la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno" los días 23, 26 y 28 de noviembre de 2018 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 S*egunda Sesión anual abierta de la Agencia Española de Protección de Datos* en enero de 2009.

6. Jornada sobre la *Introducción y aplicación de los Esquemas Nacionales de interoperabilidad y seguridad en las Administraciones Públicas* organizada por la Generalitat, Diputación de Valencia y el Club de Innovación en octubre de 2010.

7. *Tercera Sesión Anual Abierta de la Agencia Española de Protección de Datos* celebrada en octubre de 2010.

8. Seminario sobre *TIC en la Modernización de las Universidades* celebrado en marzo de 2011.

9. Seminario sobre el *Esquema Nacional de Seguridad (III): Novedades* celebrado por Socinfo SL en octubre de 2011.

10. *II Jornada Videovigilancia y Protección de Datos* celebrado por la Agencia de Protección de Datos de la Comunidad de Madrid en octubre de 2011.

11. *Congreso Nacional de Interoperabilidad y Seguridad "Una Administración más segura y conectada"* organizado por Club de Innovación en febrero de 2012.

12. Jornada de la *Comisión Intersectorial de Secretarios y TIC sobre los Esquemas Nacionales de Seguridad e Interoperabilidad*, celebrada en Cartagena, en abril de 2013.

13. 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.

14. 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.

15. Seminario *"Protección de datos y nuevas tecnologías"*, celebrado en Santander del 30 de junio al 4 de julio de 2014.

16. Curso "*Bienestar Psicoemocional y Salud Laboral"* organizado e impartido por la Gerencia de la UNED, con una duración de 3 horas lectivas el 16 de diciembre de 2014.

17. Jornada "P*rotección 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.

18. Curso "*Gestión inteligente de Redes Sociales"* impartido por El Instituto Nacional de Administración Pública (INAP) el 17 de marzo de 2015 con una duración de 7 horas lectivas.

19. Séptima Sesión Anual Abierta de la Agencia Española de Protección de Datos (AEPD) el 21 de abril de 2015.

20. XIII *Curso de Régimen Jurídico de las Universidades* celebrado en la Universidad de Castilla-La Mancha durante los días 28 y 29 de mayo de 2015.

21. Curso *"Iniciación a la Administración Electrónica"* organizado e impartido por la Gerencia de la UNED del 21 al 23 de septiembre de 2015 con una duración de 6 horas lectivas, dentro del Plan de formación del Personal de Administración y Servicios de la UNED.

22. Jornada *"Las Leyes 39&40: implicaciones para las Universidades"*, con una duración de 5 horas, organizado por AEDUN Y PwC, y celebrado en Madrid el día 20 de noviembre de 2015.

23. *Jornada informativa sobre la Nueva Ley de Procedimiento Administrativo*, de cuatro horas de duración, celebrada por la Oficina de Cooperación Universitaria el 1 de diciembre de 2015.

24. *IX Jornadas STIC CCN-CERT, detección e intercambio, factores clave, organizadas por el* CENTRO CRIPTOLÓGICO NACIONAL y celebradas en Madrid, los días 10 y 11 de diciembre de 2015, con una duración total de 12 horas.

25. Evento TIC: *Transparencia y Participación ciudadana (7),* celebrada en Madrid el 5 de abril de 2016.

26. Curso "*La transparencia en la AGE, experiencia desarrollada y líneas de mejora: nueva configuración y gestión del Portal"*, organizado por el Instituto Nacional de Administración Pública (INAP) los días 6 y 7 de junio de 2016, con una duración de 10 horas lectivas.

27. XII Seminario sobre Aspectos Jurídicos de la Gestión Universitaria, celebrado en la Universitat Pompeu Fabra los días 30 de junio y 1 de julio de 2016.

28. Evento TIC *Retos legales (2): Impacto tecnológico de las Leyes 39 y 40 en el Procedimiento Administrativo; Carpeta Ciudadana*, celebrado en Madrid el día 15 de septiembre de 2016.

29. Curso "La Reforma Legal del Régimen Administrativo. Principales novedades de las Leyes 39 y 40/2015", impartido en el Campus de Getafe de la Universidad Carlos III de Madrid los días 12, 13, 19 y 20 de septiembre de 2016, con una duración de veinte horas lectivas.

30. Encuentro de personal de las Universidades: *"E-Juristas: más allá de la tecnología legal"*, celebrado en La Coruña por la Universidad Internacional Menéndez Pelayo del 3 al 4 de noviembre de 2016, con un total de quince horas lectivas.

31. Evento TIC *"Datacenter y Ciberseguridad en AAPP (11)",* celebrado en Madrid el miércoles, 8 de febrero de 2017.

32. Evento TIC *"Nuevas obligaciones de Protección de Datos en Administraciones Públicas (5)",* celebrado en Madrid el jueves, 18 de mayo de 2017.

33. Evento TIC "Ciberseguridad (12): Defensa ante ciberataques masivos. Control de seguridad y respuesta ante ransomware, software vulnerable y agresiones inéditas" celebrado en Madrid el jueves, 13 de julio de 2017.

34. Jornada "Reformas legislativas en materia de Protección de Datos: El Reglamentos Europeo y la nueva Ley Orgánica de Protección de Datos" celebrada el día 20 de octubre de 2017 en el Auditorio del Canal de Isabel 11, en horario de 09:00 h a 15:00 h.

35. Grupos de trabajo y las "Jornadas Técnicas de RedIRIS 2018" celebradas los días 8, 9 y 10 de mayo en la Hospedería Arzobispo Fonseca de la Universidad de Salamanca, organizadas por la Entidad Pública Empresarial Red.es y RedIRIS, red española de I+D+i, con la colaboración de la Universidad de Salamanca.

36. Seminario "El Reglamento General de Protección de Datos: orientaciones para su aplicación" celebrado en la Universidad Internacional Menéndez Pelayo, del 2 al 4 de julio de 2018, con un total de dieciocho horas lectivas.

37. Ha participado en la "Mesa Redonda: Retos de los DPO/DPD" en la "Cumbre 2018 RGPD/LOPD/DPD/DPO ¿Preparados para el cambio?" organizada por la ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (QAEC) el 7 de febrero de 2018.

38. Ha asistido a la sesión solemne conmemorativa del Aniversario de la Agencia española de Protección de Datos así como a la presentación del libro "25 años de la AEPD: acompañando al ciudadano en su transformación digital" el 13 de noviembre de 2018.

39. Ha asistido a las XII Jornadas STIC CCN-CERT, celebradas en Madrid, los días 12 y 13 de diciembre de 2018.

40. Ha participado en la Mesa Redonda de la "Jornada AEPD/Delegados de Protección de Datos de Universidades" organizada por la Agencia española de Protección de Datos en su sede de Madrid, el 20 de febrero de 2019.

BICI
Curso 2017-2018
30 de enero de 2018
Número 15 / Anexo I
Boletín Interno de Coordinación Informativa

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

PREÁMBULO 3

TÍTULO PRELIMINAR. Objeto y ámbito de aplicación 4
- **Artículo 1.** *Objeto del Reglamento* 4
- **Artículo 2.** *Ámbito de aplicación* 4

TÍTULO I. Uso de los Sistemas de Información 4
- **Artículo 3.** *Uso de los Sistemas de Información* 4
- **Artículo 4.** *Uso de los equipos informáticos y cualquier otro dispositivo* 4
- **Artículo 5.** *Uso de la red corporativa* 5
- **Artículo 6.** *Uso de la Información* 6

TÍTULO II. Control de accesos 7
- **Artículo 7.** *Acceso a aplicaciones y servicios* 7
- **Artículo 8.** *Datos de carácter personal* 7

TÍTULO III. Incidencias de seguridad de la Información 7
- **Artículo 9.** *Incidencias de seguridad de ficheros automatizados* 7
- **Artículo 10.** *Incidencias de seguridad de ficheros no automatizados o en papel* 8
- **Artículo 11.** *Comunicación de incidencias que afecten a la seguridad del Sistema de Información* 8

Disposición final primera. Incumplimiento del Reglamento 8

Disposición final segunda. Entrada en vigor 8

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 o 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, 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)

Universidad Nacional de Educación a Distancia
c/ Bravo Murillo 38
28015 Madrid

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 5

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 confidencial. 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, serán tratados en calidad de responsable de tratamiento por la UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

(UNED) c/ Bravo Murillo, 38, 28015-MADRID-, con la finalidad de mantener el contacto con usted. La base jurídica que legitima este tratamiento, será su consentimiento, el interés legítimo o la necesidad para gestionar una relación contractual o similar. En cualquier momento podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación al tratamiento o portabilidad de los datos 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

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)

Universidad Nacional de Educación a Distancia
c/ Bravo Murillo, 38
28015 Madrid

ÍNDICE

1.- OBJETO 3

2.- ALCANCE 3

3.- MEDIDAS DE SEGURIDAD 3

4.- NORMATIVA 5

5.- FUNCIONES Y RESPONSABLILIDADES 5

6.- CONTRATACIÓN DE EMPRESAS ESPECIALIZADAS 6

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.

3.- MEDIDAS DE SEGURIDAD A ADOPTAR EN EL DESECHADO O DESTRUCCIÓN DE DOCUMENTOS

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.

Al respecto, el Reglamento General Europeo de protección de datos, de 2016 (en adelante RGPD) señala en su artículo 5, relativo a los Principios del tratamiento, lo siguiente:

Los datos personales serán:

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

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

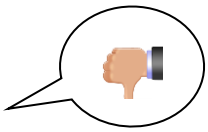
La normativa europea relativa a la protección de datos exige una serie de niveles de seguridad en la

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 Infraestructura y 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 **trituración** 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

- ✓ 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.

- ✓ LEY ORGÁNICA 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

- ✓ 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)

- ✓ NORMATIVA PROPIA DEL ARCHIVO GENERAL DE LA UNED

5.-FUNCIONES Y RESPONSABILIDADES

Responsable del Tratamiento
El Responsable del Tratamiento tendrá las siguientes funciones:

1. 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.

2. Mantener el correcto estado de los armarios, archivos y dependencias que contienen los documentos, en cuanto a la seguridad y privacidad de la información de carácter personal.

3. Establecer los permisos de los usuarios con acceso autorizado a los armarios, archivos y dependencias citados.

4. 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 en materia de protección de datos.

5. 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 Tratamiento adoptará aquellas que impidan el acceso de personas no autorizadas.

6. Mantener informado al usuario para efectuar una entrada o salida de archivos en papel.

Responsable de Seguridad
Es competente para llevar a cabo las funciones de control relativas a garantizar el cumplimiento de las medidas de seguridad para documentos en papel.

Gestor de Tratamiento
Sus funciones y obligaciones son las mismas que las del Responsable del Tratamiento, delegadas por éste.

Usuario

Cumplir con las obligaciones respecto al tratamiento, manipulación, reutilización o desechado de los documentos 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 4.4.

PROCEDIMIENTO PARA DAR DE BAJA DISPOSITIVOS HARDWARE

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

Universidad Nacional de Educación a Distancia
c/ Bravo Murillo,38
28015-Madrid

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

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

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/Dª: _____

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/Dª: _____, como Responsable del Servicio de la UNED autorizo al Técnico Informático D/Dª: _____ _____ a acceder al ordenador del puesto de trabajo del usuario D/Dª: _____ 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.

NORMATIVA DE LA GESTIÓN DE INCIDENTES Y VIOLACIONES DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Universidad Nacional de Educación a Distancia
Avenida de Esparta, 9. Ctra. Del Escorial, Km 5
28232 Las Rozas, Madrid

ÍNDICE

1. OBJETO DEL DOCUMENTO 3
2. ALCANCE 3
3. ACRÓNIMOS Y DEFINICIONES 3
4. INTRODUCCIÓN 5
5. NORMATIVA APLICABLE 6
6. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES 7
6.1 Detección y notificación 7
6.2 Registro 7
6.2.1 Categorización inicial de incidentes según su impacto 8
6.2.1.1 Nivel BAJO 8
6.2.1.2 Nivel MEDIO 8
6.2.1.3 Nivel ALTO 9
6.3 Gestión del incidente y recopilación de evidencias 9
6.3.1 Gestión de incidentes de nivel Medio y Alto 10
6.3.2 Registro de la gestión de incidentes nivel Medio y Alto [op.exp.9] 10
6.4 Recopilación de evidencias 11
6.5 Gestión del incidente, cierre 11
6.6 Aprendizaje 12
6.7 Concienciación de medidas de protección personal 3 del ENS [mp.per.3] 12
6.8 Formación de medidas de protección personal 4 del ENS [mp.per.4] 12
ANEXO I. MARCO LEGAL 13
ANEXO II. PROCEDIMIENTO DE NOTIFICACIÓN AL CCN-CERT 21
ANEXO III. METRICAS CIERRE 22
Sistema de métricas [op.mon.2] 22
ANEXO IV. REFERENCIAS 23

1. OBJETO DEL DOCUMENTO

El presente documento tiene como objeto definir la normativa, así como de los requisitos de los procedimientos a los que servirá de marco y referencia, aplicables a la Gestión de incidencias en la Universidad Nacional de Educación a Distancia, en adelante UNED, principalmente dentro del alcance marcado en el 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, en adelante ENS. Se atiende, especialmente, a las previsiones contempladas en dicha norma y otras que la condicionan y complementan, recogidas en el punto 5 y ampliadas en el ANEXO I del presente documento.

En concreto el artículo 11 del ENS señala la obligación de que las Entidades Públicas, en su ámbito de aplicación, dispongan de una Política de Seguridad de la Información que articule una serie de Requisitos Mínimos de Seguridad. Entre tales requisitos se contempla la Gestión de incidentes de Seguridad, exigencia que se concreta en el artículo 24 del mismo cuerpo legal, que señala que:

- *Se establecerá un sistema de detección y reacción frente a código dañino.*
- *Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.*

Esta norma, al igual el Reglamento General de Protección de Datos, establece la necesidad no solo de gestionar los incidentes de seguridad, sino también la obligación de comunicar los incidentes graves a la autoridad competente y si se hubieran visto gravemente afectados datos personales, a sus propietarios y a la Agencia Española de Protección de Datos, en los casos legalmente previstos.

2. ALCANCE

El alcance de la presente normativa es de aplicación en todos los ámbitos de la UNED, donde sean de aplicación la Política de Seguridad de la Información y la Normativa de Seguridad.

Siendo, por tanto, de aplicación en todas las instalaciones de la UNED en las que se desarrollen actividades utilizando medios electrónicos, especialmente aquellas que tengan como objeto prestar un servicio a los ciudadanos. Será de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Universidad, incluyendo, en su caso, proveedores externos, especialmente cuando sean usuarios de los Sistemas de Información.

3. ACRÓNIMOS Y DEFINICIONES

TÉRMINO	DEFINICIÓN
Incidente de seguridad	Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información y de la información.
Usuario	Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

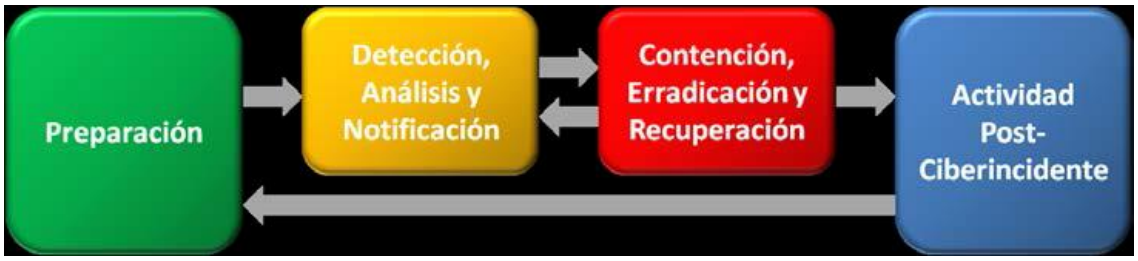
Ciberincidente	Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y de la información que trata o los servicios que presta.
Violación de seguridad de los datos personales	Toda violación de la seguridad que ocasione la destrucción, perdida 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
ENS	Esquema Nacional de Seguridad. 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 Real Decreto 951/2015, de 23 de octubre
CCN-CERT	Centro Criptológico Nacional-Computer Emergency Response Team Organización especializada en responder inmediatamente a incidentes relacionados con la seguridad de las redes o los equipos. También publica alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misión elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan.

4. INTRODUCCIÓN

En el presente documento se definirán de forma global los procedimientos para la gestión integral de los incidentes de seguridad, los cuales recogerán:

- La definición y clasificación de los incidentes a tenor del análisis de riesgos, la naturaleza y el método de resolución.
- Los criterios y formularios para la comunicación de incidentes y, en su caso, el intercambio de información, interna y externa.
- El nivel de peligrosidad de los incidentes.
- Los procedimientos operativos de seguridad.
- Los mecanismos para la notificación de informes de incidentes.

Asimismo, en dichos procedimientos se debe especificar la posición del Equipo de Respuesta a incidentes, sus competencias y autoridad dentro de la estructura de la organización y la definición de los roles y responsabilidades de cada unidad, departamento y persona dentro del Plan de Respuesta a incidentes.



Plan de Respuesta a incidentes

Estas fases se transpondrán en procedimientos específicos por tipo de ataque, que tendrán el mismo esquema o método de resolución:

- Detección y notificación.
- Registro
- Gestión, contención y recopilación de evidencias
- Cierre del incidente
- Aprendizaje y mejora

Igualmente, en aplicación del ENS se deberá:

- Redactar y aprobar normas técnicas sobre la custodia de las evidencias de un incidente.
- Informar y concienciar a todos los usuarios de los mecanismos de notificación.
- Notificación de incidentes al CCN-CERT*.

* El Artículo 36 del ENS, indica la obligación de las Administraciones Públicas de notificar al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información tratada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo III del presente documento.

5. NORMATIVA APLICABLE

Las diferentes regulaciones legales y referencias que condicionan la presente normativa están desarrolladas en el ANEXO I del presente documento.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en adelante **RGPD**
- Reglamento (UE) nº 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas
- 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 Real Decreto 951/2015, de 23 de octubre, en adelante **ENS**
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en adelante **Ley 39/2015**
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en adelante **Ley 40/2015**
- RESOLUCIÓN DE LA SECRETARÍA DE ESTADO DE FUNCIÓN PÚBLICA POR LA QUE SE APRUEBA LA INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

OTROS DOCUMENTOS DE INTERÉS

- Documentos y Guías CCN-STIC, en especial:
  - Guía CCN-STIC 403 Gestión de Incidentes de Seguridad.
  - Guía CCN-STIC 817 Gestión de Ciberincidentes en el ENS.
  - Guía CCN-STIC-821 Normas de seguridad en el ENS.
  - El Anexo I de la Guía CCN-STIC-822 Procedimientos de seguridad en el ENS.
- CERTSI RFC 2350 – Punto 6 Modelo de notificación de incidentes.
- Normas ISO. ISO/IEC 27001:2013 e ISO/IEC 27035:2016

6. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

El plan de acción para gestionar los incidentes se recogerá en el **Procedimiento de Gestión de Incidentes y violaciones de seguridad de los datos personales**, el cual además de resolverlos según su nivel y naturaleza, incorporará medidas que permitan conocer la calidad del sistema de protección y de detección de patrones.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en el procedimiento específico para la resolución de incidentes de esta naturaleza recogido en el presente documento.

Todos los incidentes se clasificarán en uno de los siguientes estados:

- Abierto: el incidente ha sido comunicado y dado de alta.
- En proceso o trámite: el incidente está siendo tratado y está en fase de resolución.
- Suspendido: en espera de alguna herramienta o investigación.
- Cerrado: el incidente ha sido resuelto o cerrado.

6.1 Detección y notificación

Cualquier usuario que tenga conocimiento de una incidencia, o debilidad de seguridad, deberá notificarla de forma inmediata a través de los canales y destinatarios establecidos. Por lo que es imprescindible que todos los usuarios (internos y externos) sean informados y concienciados sobre la responsabilidad de notificar las incidencias de seguridad de forma inmediata, así como sobre los procedimientos y canales de comunicación disponibles para ello.

6.2 Registro

En el registro de las incidencias de seguridad, habrá que tener en cuenta las siguientes consideraciones:

- Todas las incidencias de seguridad deben tener un número único que permita su identificación y trazabilidad a lo largo del proceso de gestión.
- Toda la información relacionada con las causas, tratamiento y resolución de incidencias de seguridad debe estar correctamente registrada junto con las evidencias, log y trazas que hayan sido obtenidos sobre la misma.
- La información registrada debe ser almacenada y protegida de forma que no pueda ser modificada (incluso por los administradores del sistema).
- En caso de que la incidencia afecte a tratamientos que contengan datos de carácter personal, se deberá tener en cuenta el procedimiento específico del presente documento.
- El Registro de Incidencias contendrá, al menos, los siguientes campos de información:
    - Tipo de incidencia.
    - Momento en que se ha producido, o en su caso detectado.
    - Persona que realiza la notificación.
    - Persona que recibe la notificación.

- Persona a quién se comunica la notificación.
- Efectos de la Incidencia.
- Medidas correctoras aplicadas.
- Si se han visto afectados tratamientos que contengan datos personales: persona que ejecutó el proceso de recuperación de datos, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente (esto se aplicará cuando la incidencia afecte a datos de nivel medio o alto).

6.2.1 Categorización inicial de incidentes según su impacto

Después de quedar registrado el incidente se determinará su nivel inicial según el tipo de amenaza y el impacto que haya ocasionado. Se aplicarán diferentes procedimientos según el nivel de peligrosidad. Este último se determinará al cierre de la incidencia, o durante su contención, en cinco niveles según lo dispuesto en el ANEXO III del presente documento. Los incidentes de nivel alto, muy alto o crítico deberán ser notificados al CCN-CERT según lo dispuesto en el ANEXO II "**Procedimiento de notificación al CCN-CERT"**.

En cuanto al impacto, una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

6.2.1.1 Nivel BAJO

Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la Organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1. La reducción de forma apreciable de la capacidad de la Organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
2. El sufrimiento de un daño menor de los activos de la Organización.
3. El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4. Causar un perjuicio menor a algún individuo, que aun siendo molesto pueda ser fácilmente reparable.
5. Otros de naturaleza análoga.

6.2.1.2 Nivel MEDIO

Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad, supongan un perjuicio grave sobre las funciones de la Organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

1. La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.

2. El sufrimiento de un daño significativo por los activos de la Organización.

3. El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.

4. Causar un perjuicio significativo a algún individuo, de difícil reparación.

5. Otros de naturaleza análoga.

6.2.1.3 Nivel ALTO

Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la Organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1. La anulación de la capacidad de la Organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
2. El sufrimiento de un daño muy grave, e incluso irreparable, de los activos de la Organización.
3. El incumplimiento grave de alguna ley o regulación.
4. Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5. Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

6.3 Gestión del incidente y recopilación de evidencias

Los incidentes de seguridad serán gestionados según lo dispuesto en el Procedimiento de Gestión de Incidentes, de acuerdo con su naturaleza y nivel. Teniendo siempre en cuenta las siguientes consideraciones:

- Los responsables de la gestión de las incidencias deberán recabar de los usuarios toda la información necesaria para gestionarlas.

- En el Procedimiento de Gestión de Incidentes, se establecerán las responsabilidades y procesos necesarios para garantizar una respuesta rápida, efectiva y ordenada a las incidencias y debilidades de seguridad.

- En determinados casos será necesario adoptar medidas para la contención de la incidencia que eviten daños mayores. En aquellos casos en que la adopción de estas medidas de contención conlleve una paralización de los sistemas, se debe informar con la

mayor antelación posible a los usuarios afectados mediante los canales de comunicación que hayan sido formalmente establecidos en el Procedimiento de Gestión de Incidentes.

- En los casos de incidencias graves o en las que sea necesario activar el Plan de Contingencias, estas deben ser comunicadas de forma inmediata al Responsable de Seguridad, que debe decidir las acciones a adoptar en cada caso (entre ellas la activación del Plan de Contingencias o la convocatoria del Comité de Seguridad para informar de los hechos).

- La resolución de la incidencia debería ser comunicada a los usuarios que la han reportado o que fueron afectados durante su gestión, al proceder al cierre definitivo de la misma.

6.3.1 Gestión de incidentes de nivel Medio y Alto

Si el impacto inicial del incidente es de nivel Medio o Alto, según lo dispuesto en la **medida de explotación 7 del marco operacional** del ENS, denominada **op.exp.7**, se deberá disponer de un proceso integral para hacer frente a este tipo de incidentes en la seguridad del sistema, incluyendo:

a) Procedimiento de comunicación de eventos de seguridad y debilidades, detallando los criterios de clasificación, de no existir y debido a la necesidad de realizar el escalado de la notificación al CCN-CERT se seguirá lo dispuesto en el ANEXO III del presente documento.

b) Procedimiento para la adopción de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d) Procedimientos para informar a las partes interesadas, internas y externas.

e) Procedimientos destinados a:

- Prevenir que se repita el incidente.
- Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
- Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

6.3.2 Registro de la gestión de incidentes nivel Medio y Alto [op.exp.9]

Se registrarán todas las actuaciones relacionadas con la gestión de estos incidentes, de forma que:

a) Se registrarán en el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

b) Se registrarán aquellas evidencias que puedan, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución

de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.

c) Como consecuencia del análisis de los incidentes, se revisará que eventos son auditables en vistas de mejorar la recopilación de evidencias.

6.4 Recopilación de evidencias

En general, siempre es conveniente empezar el acopio de evidencias tan pronto como se detecta un incidente. Por otro lado, desde un punto de vista probatorio, es conveniente obtener inmediatamente una instantánea del sistema atacado, dejándolo inaccesible y garantizando su integridad, antes de tratar las copias hechas del sistema atacado con diferentes tipos de herramientas que, de otro modo, podrían alterar parte de la información o el estado de los sistemas comprometidos.

Por lo que procurará mantener un registro detallado de todas las evidencias, incluyendo:

- La identificación de la información (por ejemplo, la localización, el número de serie, número de modelo, el nombre del sistema, dirección MAC (identificador de la tarjeta o sistema de res) y direcciones IP de los ordenadores afectados.
- Nombre, cargo y el teléfono de cada persona que ha recogido o gestionado evidencias durante la investigación del incidente.
- Fecha y hora de cada ocasión en la que ha sido tratada cada evidencia.
- Ubicaciones donde se custodiaron las evidencias.

6.5 Gestión del incidente, cierre

Para poder dar por cerrado un incidente de seguridad, además de haberse controlado, debemos responder a las siguientes preguntas:

En la fase de Registro y durante la resolución:

- ¿QUÉ ha sucedido o CUÁLES son los signos de alerta?
- ¿DÓNDE ha ocurrido?
- ¿CUÁNDO se produjo?
- ¿CÓMO o en qué circunstancias?
- ¿POR QUÉ se ha producido o CUÁL es su origen?

En el cierre, una vez analizado el alcance del incidente, se especificará:

- Nivel de Peligrosidad (final) del incidente.
- Resumen de las acciones realizadas para:
  - Contención del incidente
  - Erradicación del incidente
  - Recuperación de los sistemas afectados
- Impacto del incidente, medido en:
  - Número de equipos afectados
  - Valoración del impacto en la imagen pública del Organismo
  - Dimensión (Confidencialidad, Integridad, Disponibilidad, Autenticación, Trazabilidad, Legalidad) de la seguridad afectada
  - Porcentaje de degradación sufrido en los servicios ofrecidos a los ciudadanos
  - Porcentaje de degradación sufrido en los servicios internos del Organismo

- Valoración del coste directamente imputable al incidente:
  - En horas de trabajo
  - Coste de compra de equipamiento o software necesario para la gestión del incidente
  - Coste de contratación de servicios profesionales para la gestión del incidente

- Conclusión: Elaboración de las conclusiones finales, que permitirán mejorar la seguridad.

6.6 Aprendizaje

En el aprendizaje es fundamental, para evitar futuros incidentes de naturaleza similar, tener en cuenta las siguientes consideraciones:

• El registro de las incidencias de seguridad debe ser revisado periódicamente, para identificar incidentes recurrentes, posibles deficiencias de seguridad o proponer las soluciones más adecuadas. Se debería elaborar un informe donde se establezcan las conclusiones de las revisiones realizadas, en vistas de una mejora continua de la seguridad.

• La evaluación de las incidencias de seguridad de la información puede indicar la necesidad de aumentar o añadir nuevos controles que limiten la frecuencia, daño o coste de futuras incidencias o pueden ser tenidos en cuenta como fuente de información dentro de los procesos de revisión de las políticas de seguridad.

• El responsable y los operadores de incidencias, así como, en su caso, los usuarios afectados deben ser formados y prevenidos sobre la base de conocimiento adquirido, y sobre posibles incidencias que puedan repetirse en el futuro para prevenir que estas vuelvan a producirse. De este modo, salvando los aspectos de confidencialidad propios de la gestión de incidencias, éstas deben ser utilizadas dentro de los procesos de mejora continua, como ejemplo para la concienciación y formación de los usuarios y administradores del sistema ante incidencias similares de modo que pueda prevenirse su reaparición en el futuro.

6.7 Concienciación de medidas de protección personal 3 del ENS [mp.per.3]

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

En particular, se recordará regularmente:

a) La normativa de seguridad relativa al buen uso de los sistemas.

b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

6.8 Formación de medidas de protección personal 4 del ENS [mp.per.4]

Se formará regularmente al personal en aquellas materias que se requieran para el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.

b) Detección y reacción a incidentes.

c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

ANEXO I. MARCO LEGAL

Esquema Nacional de Seguridad

Relación de artículos del Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad, actualizados por el RD951/2015.

Artículo 7. Prevención, reacción y recuperación.

3. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

4. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

Artículo 8. Líneas de defensa.

1. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

Artículo 11. Requisitos mínimos de seguridad.

1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:
…
k) Prevención ante otros sistemas de información interconectados

l) Registro de actividad

m) Incidentes de seguridad

n) Continuidad de la actividad

o) Mejora continua del proceso de seguridad

Artículo 24. Incidentes de seguridad

1. Se establecerá un sistema de detección y reacción frente a código dañino.

2. Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Capítulo VII Respuesta a incidentes de seguridad

Artículo 36. Capacidad de respuesta a incidentes de seguridad de la información.

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I del presente real decreto.

Artículo 37. Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.

1. De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones públicas.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes de auditoría de los sistemas afectados, registros de auditoría, configuraciones y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y su normativa de desarrollo, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.

c) Formación destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las Administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquél, será coordinador a nivel público estatal.

Artículo 43. Categorías.

1. La categoría de un sistema de información, en materia de seguridad, modulará el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.

2. La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I.

3. La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Disposición adicional cuarta. Desarrollo del Esquema Nacional de Seguridad.

1. Sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica según lo establecido en el artículo 29, apartado 2, se desarrollarán las siguientes instrucciones técnicas de seguridad que serán de obligado cumplimiento por parte de las Administraciones públicas:

a) Informe del estado de la seguridad.

b) Notificación de incidentes de seguridad.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

El marco legal que regula el tratamiento de datos de carácter personal es el siguiente:

Disposición adicional novena. Tratamiento de datos personales en relación con la notificación de incidentes de seguridad

Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

RGPD Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016

El RGPD, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), regula en los considerandos 85, 86, 87 y 88 y en los artículos 32, 33 y 34, la seguridad del tratamiento así como la necesidad de comunicar, por parte del Delegado de Protección de Datos, los incidentes a las Autoridades de control y si procede al interesado.

Considerandos 85, 86, 87 y 88

"(85)Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en

cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

(88) Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido.

Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales."

***Artículo 32.** Seguridad del tratamiento*

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) *la seudonimización y el cifrado de datos personales;*
b) *la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
c) *la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
d) *un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 33. *Notificación de una violación de la seguridad de los datos personales a la autoridad de control*

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34. *Comunicación de una violación de la seguridad de los datos personales al interesado*

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

OTROS DOCUMENTOS DE INTERÉS

Normas ISO. ISO/IEC 27001:2013 e ISO/IEC 27035:2016

La gestión de incidentes de seguridad y buenas prácticas. En concreto, dos referencias claras:

ISO/IEC 27001:2013, que dedica el bloque de control 16, Gestión de incidentes de seguridad y que incluye los siguientes controles:

1.1 Responsabilidades y procedimientos: Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

1.2 Notificación de los eventos de seguridad de la información: Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.

1.3 Notificación de puntos débiles de la seguridad: Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.

1.4 Valoración de eventos de seguridad de la información y toma de decisiones: Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.

1.5 Respuesta a los incidentes de seguridad: Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.

1.6 Aprendizaje de los incidentes de seguridad de la información: Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.

1.7 Recopilación de evidencias: La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

ISO/IEC 27035:2016, que se centra en la gestión de incidentes de seguridad.

ANEXO II. PROCEDIMIENTO DE NOTIFICACIÓN AL CCN-CERT

Una vez detectado un ataque deberá determinarse su clase y tipo, según las tablas de criterios de determinación de nivel de peligrosidad e impacto de los ciberincidentes de la Guía CCN-STIC 817 GESTIÓN DE CIBERINCIDENTES. Resultando el nivel en cinco valores: bajo, medio, alto, muy alto y crítico.

En el artículo 36 del ENS se indica la obligación de las Administraciones Publicas de comunicar al CCN-CERT los incidentes de seguridad cuando sean categorizados al menos como de peligrosidad alta. Asimismo, en el RD951/2015 a dicho artículo se añade un segundo párrafo indicando la obligación de informar de aquellos que tengan un impacto significativo.

El artículo 37, el apartado 1.a) también es actualizado por el RD951/2015, delimita las funciones del CCN-CERT, el cual a través de su servicio soporte dará apoyo técnico y de coordinación, ante cualquier agresión recibida en los sistemas de información de las Administraciones Públicas.

Para el cumplimiento de los fines indicados en los párrafos anteriores, se podrá recabar cualquier tipo de información que se considere relevante para la investigación del incidente de los sistemas afectados. La comunicación de datos, si contienen datos personales se efectuará con pleno consentimiento de lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de Protección de Datos Personales (RGPD). Actuando la UNED como cedente y el CCN-CERT como cesionario, ya que las dos actúan en cumplimiento de fines relacionados con su función pública no será preciso el consentimiento del afectado, según lo dispuesto en el artículo 6.1.f) del RGPD.

La comunicación de información de datos de carácter institucional u organizativo a la que se refiere el artículo 37.1.a) último párrafo, del ENS, será suministrada y comunicada en función de su confidencialidad, atendiendo a lo dispuesto en el artículo 43 y Anexo I, en relación con el citado artículo 37.1.a) del ENS.

ANEXO III. METRICAS CIERRE

El artículo 35 del ENS indica la obligación de mandar al CCN-CERT un informe estadístico, al menos anualmente, con los ciberincidentes registrados.

Se deberá seguir las indicaciones de la guía CCN-STIC 817, para calcular las métricas de implantación, de eficacia y de eficiencia, con objeto de mejorar la Gestión de los Ciberincidentes.

Para poder calcular dichas métricas, según la categoría del sistema y sus dimensiones de seguridad, se han de recopilar de acuerdo a la siguiente tabla:

Sistema de métricas [op.mon.2]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA:

Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II del ENS y, en su caso, para proveer el informe anual requerido por el artículo 35 del ENS.

Categoría MEDIA:

Además, se recopilarán datos para valorar el sistema de gestión de incidentes, permitiendo conocer

– Número de incidentes de seguridad tratados.

– Tiempo empleado para cerrar el 50% de los incidentes.

– Tiempo empleado para cerrar el 90% de los incidentes.

Categoría ALTA

Se recopilarán además datos para conocer la eficiencia del sistema de seguridad TIC:

– Recursos consumidos: horas y presupuesto.

ANEXO IV. REFERENCIAS

https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/respuesta-incidentes.pdf

https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

ANEXO 4.7.

PROCEDIMIENTO DE GESTION INCIDENTES Y VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES

Universidad Nacional de Educación a Distancia
c/ Bravo Murillo 38
28015 Madrid

ÍNDICE

1 OBJETO DEL DOCUMENTO 3

2 PROCEDIMIENTO DE GESTION INCIDENTES Y VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES 3

2.1 Detección y Notificación de incidentes y violaciones de seguridad de los datos personales.....3

2.2 Contenido mínimo de la notificación 4

2.3 Criterios para valorar si un incidente de seguridad debe notificarse 5

2.4 Pasos para informar a la AEPD de una brecha de seguridad 5

1 OBJETO DEL DOCUMENTO

El Reglamento General de Protección de Datos, en adelante RGPD, define como "violación de la seguridad de los datos personales": toda violación de la seguridad que ocasione la destrucción, perdida 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.

Llegado el caso de producirse, se debe actuar con agilidad y diligencia, así como mantener un registro de todas las violaciones de seguridad, sean o no objeto de notificación a la autoridad de control o comunicación al interesado, por lo que se siempre se debe comunicar internamente.

El presente documento tiene como objeto definir el procedimiento aplicable a la Gestión de incidentes y violaciones de seguridad de los datos personales en la Universidad Nacional de Educación a Distancia, en adelante UNED, dentro del alcance del Reglamento (UE) 2016/679, de 27 de abril de 2016, de Protección de Datos Personales (RGPD), así como el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS.

2 PROCEDIMIENTO DE GESTION INCIDENTES Y VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES

El proceso de gestión de incidentes y violaciones de seguridad de los datos personales contemplará las siguientes actividades:

- **Detección y comunicación interna del incidente**, así como el proceso de escalado para informar a los diferentes actores que participarán en la resolución.
- **Triaje**: valoración de los hechos, su categorización, prioridad y asignación de los responsables encargados de gestionar la respuesta.
- **Análisis**: determinar qué ha podido suceder, el impacto que ha causado o podría causar, estableciendo las acciones a emprender como respuesta.
- **Respuesta**: supone ejecutar, una vez focalizado el problema, una serie de tareas o iniciar un conjunto de protocolos que tengan como efecto la mitigación del incidente y la recuperación de la normalidad. Siempre deben incluir un análisis de causas y una incorporación de mejoras para evitar que el incidente pudiera repetirse.

2.1 Detección y Notificación de incidentes y violaciones de seguridad de los datos personales

Si se detecta, o sospecha, que existe un incidente que afecte o no a datos personales, debe ser comunicado, sin dilación, mediante el envío del **Formulario General de Comunicación de Incidentes y violaciones de seguridad de datos personales** al Centro de Tecnología de la UNED, a través del CAU, cuando no revistan la categoría de graves.

Los incidentes de seguridad graves se gestionarán por el Departamento de Comunicaciones y Seguridad del Centro de Tecnología de la UNED, bajo la dirección del Jefe de Área.

El responsable del tratamiento, una vez que tiene la certeza de que es una violación de seguridad, debe notificarlo a la autoridad de control (AEPD) en un plazo máximo de 72 horas, mediante el envío del **Formulario para comunicar a la AEPD en caso de incidente grave** cuando constituya un riesgo para los derechos y libertades de las personas. El responsable puede delegar esta tarea al Encargado de tratamiento, no obstante, no se delega la responsabilidad. Se debe informar al Delegado de Protección de Datos, pues es el punto de contacto con la AEPD.

Asimismo, se deberá comunicar a los afectados, propietarios de los datos personales, la violación si esta puede comportar un alto riesgo para sus libertades y derechos (casos en que se desvele información confidencial o contraseñas, se difundan masivamente datos sensibles o se puedan producir daños económicos, entre otros). El responsable lo deberá comunicar directamente a las personas afectadas sin dilaciones indebidas y en lenguaje claro y sencillo, excepto que:

- El responsable hubiera adoptado medidas de protección adecuadas, como que los datos no sean inteligibles para personas no autorizadas (cifrado).
- Haya aplicado medidas ulteriores que garanticen que ya no existe la probabilidad de que se concrete el alto riesgo.
- Suponga un esfuerzo desproporcionado, debiéndose sustituir por otras medidas alternativas como puede ser una comunicación pública.

Si se produjera un incidente de gran impacto se recomienda comunicarlo, sin dilación, a la autoridad de control, aunque no se tenga constancia de todo lo sucedido, sin perjuicio de que ese primer contacto se complete con una notificación formal documentada dentro del plazo de 72 horas.

Pudiera haber casos que debido a la complejidad en determinar el alcance no puedan ser comunicados en el plazo máximo, en estos casos es posible notificar con posterioridad siempre que se expliquen los motivos de la dilación de forma documentada.

2.2 Contenido mínimo de la notificación

La notificación ha de incluir un contenido mínimo:

- La naturaleza de la violación de seguridad de los datos personales, categorías y cantidad de datos, así como de interesados afectados
- El nombre y los datos de contacto del Delegado de Protección de Datos
- Las medidas adoptadas por el responsable para resolver la violación de seguridad de los datos personales
- Si procede, las medidas adoptadas para mitigar los posibles efectos negativos

2.3 Criterios para valorar si un incidente de seguridad debe notificarse

- El potencial daño para los datos de los interesados, si produce agravio emocional, físico o financiero.
- El volumen de datos personales afectados.
- El nivel de los datos personales, según la relación de las tipologías de datos considerados 'sensibles' o de especial protección.

Artículo 9 del RGPD. Categorías especiales de datos

- Opiniones políticas
- Convicciones religiosas o filosóficas
- Origen étnico o racial
- Afiliación sindical
- Datos relativos a la vida sexual o la orientación sexual
- Datos relativos a la salud
- Datos genéticos
- Datos biométricos

Asimismo, en este apartado habrá que considerar lo estipulado en el artículo 9 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2.4 Pasos para informar a la AEPD de una brecha de seguridad

1. Valoración del riesgo. Determinar si se han causado daños a los afectados en sus derechos o libertades en función de las características y tipo de datos.
2. Evaluar si hay daños materiales o inmateriales.
3. Calcular el alcance.
4. Ver si es una evidencia o un incidente real
5. Rellenar el formulario correspondiente

FORMULARIO GENERAL DE COMUNICACIÓN DE INCIDENTES Y VIOLACIONES DE SEGURIDAD	
FASE DE REGISTRO	
FECHA Y HORA DE LA NOTIFICACIÓN	Fecha Hora
DATOS DE LA PERSONA QUE LO NOTIFICA	Nombre y apellidos Departamento/Unidad/Cargo Teléfono Correo electrónico
DESCRIPCIÓN DE LA INCIDENCIA	
DESCRIPCIÓN DE LA INCIDENCIA	Fecha y hora del incidente ¿Quién lo descubre? ¿A quién lo comunica? Tipología (elija uno o varios elemento de la lista siguiente): ☐ daños físicos Hardware ☐ incumplimiento o violación de requisitos y regulaciones legales ☐ fallos en las configuraciones ☐ denegación de servicio ☐ acceso no autorizado, espionaje y robo de información ☐ borrado o pérdida de información ☐ infección por código malicioso

	Descripción de la incidencia: origen, fuente, causa e intencionalidad: **Ubicación del incidente:** **Descripción del sistema (Sistema Operativo-Versión, Nivel de parcheado, Software instalado/servicio, otros de interés):** **Afecta a datos personales, en caso afirmativo indicar si son estos sensibles**

CIERRE INCIDENCIA	
NÚMERO DE TICKET	
FECHA Y HORA DE LA RESOLUCIÓN	**Fecha:** **Hora:**
NIVEL DE PELIGROSIDAD (FINAL) DEL INCIDENTE	
RESUMEN DE LAS ACCIONES REALIZADAS PARA:	**1.- Contención del incidente (descripción resumida en el siguiente cuadro):** **2.- Erradicación del incidente (descripción resumida en el siguiente cuadro):** **3.- Recuperación de los sistemas/datos afectados (descripción resumida en el siguiente cuadro):**
EVIDENCIAS RECOGIDAS/ANÁLISIS FORENSE	

IMPACTO DEL INCIDENTE MEDIDO EN:	**1.- Número de equipos afectados:** **2.- Valoración del impacto en la imagen pública del Organismo:** **3.- Dimensión (Confidencialidad, Integridad, Disponibilidad, Autenticación, Trazabilidad, Legalidad) de la seguridad afectada:** **4.- Porcentaje de degradación sufrido en los servicios ofrecidos a los ciudadanos:** **5.- Porcentaje de degradación sufrido en los servicios internos del Organismo:** **6.- Valoración del coste directamente imputable al incidente:** **7.- En horas de trabajo:** **8.- Coste de compra de equipamiento o software necesario para la gestión del incidente:** **9.- Coste de contratación de servicios profesionales para la gestión del Incidente:**

MEDIDAS ADOPTADAS PARA RESOLVER Y PREVENIR	
CONCLUSIÓN: Elaboración de Las conclusiones finales que permitirán mejorar la seguridad	

FORMULARIO PARA COMUNICAR A LA AEPD EN CASO DE INCIDENTE GRAVE	
1.- IDENTIDAD DEL RESPONSABLE DEL TRATAMIENTO	
2.- IDENTIDAD Y DATOS DEL DELEGADO DE PROTECCIÓN DE DATOS	
3.- SE TRATA DE UNA PRIMERA O SEGUNDA NOTIFICACIÓN	
4.- FECHA Y HORA DEL INCIDENTE (SI SE CONOCEN; EN CASO NECESARIO, PUEDE EFECTUARSE UNA ESTIMACIÓN) Y DE DETECCIÓN DEL INCIDENTE	
5.- TIPO DE VIOLACIÓN:	**(Elija uno o varios elementos de la siguiente lista):** ☐ **daños físicos Hardware** ☐ **incumplimiento o violación de requisitos y regulaciones legales** ☐ **fallos en las configuraciones** ☐ **denegación de servicio** ☐ **acceso no autorizado, espionaje y robo de información** ☐ **borrado o pérdida de información** ☐ **infección por código malicioso** ☐ **otros**

6.- NATURALEZA Y CONTENIDO DE LOS DATOS PERSONALES	**1.- Categoría datos especiales afectados: (Opinión política, Religión, Origen étnico o racial, Afiliación sindical, vida u orientación sexual, Salud, genéticos, biométricos, económicos)** **2.- Otras categorías de datos afectados:** **Cantidad de datos (número):** **Interesados afectados (número):** **El potencial daño para los datos, ¿produce a los afectados agravio emocional, físico o financiero?** ☐ **SI** ☐ **NO** **Los datos personales afectados, ¿están seudomizados?:** ☐ **SI** ☐ **NO**
7. MEDIDAS TÉCNICAS Y DE ORGANIZACIÓN QUE SE HAN APLICADO A LOS DATOS PERSONALES	
8. RESUMEN DEL INCIDENTE QUE HA CAUSADO LA VIOLACIÓN DE DATOS PERSONALES (INDICACIÓN DE LA UBICACIÓN FÍSICA DE LA VIOLACIÓN Y DEL SOPORTE DE ALMACENAMIENTO)	
9. MEDIDAS TÉCNICAS Y DE ORGANIZACIÓN QUE HA ADOPTADO PARA PALIAR LOS EFECTOS NEGATIVOS	

10. SI SE HA COMUNICADO A LOS AFECTADOS	**Contenido de la notificación** **Medios de comunicación utilizados** **Número de afectados a los que se ha remitido la notificación** **Algún afectado es ciudadano de otro Estado miembro del a UE.**
11. SE HA REALIZADO NOTIFICACIÓN A OTRAS AUTORIDADES NACIONALES COMPETENTES o CERTs, EN CASO DE RIESGO PARA LOS DERECHOS Y LIBERTADES DE LAS PERSONAS FÍSICAS	**En caso afirmativo consigne:** ☐ **Antes de 72 horas** ☐ **Más de 72 horas indicando los motivos**

ANEXO 4.8.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNED

(Aprobada por el Consejo de Gobierno el 13 de diciembre de 2016)

(Actualizada, el 4 de febrero de 2019, por el Comité de Seguridad de la Información)

Universidad Nacional de Educación a Distancia
c/ Bravo Murillo 38
28015 Madrid

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
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 y que deroga la Directiva 95/46/CE
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 y completar sus disposiciones. Garantizar los derechos digitales de los ciudadanos según lo establecido en el art. 18.4 de la Constitución Española
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, en tanto no se oponga a la Ley 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales
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 Tecnología	
Director de Recursos Humanos	Responsable del Servicio
Jefe de Área de Sistemas y Bases de datos	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	Delegada de Protección de Datos
Jefe de Área de Comunicaciones y Seguridad	Responsable de Seguridad de la Información
Asesor de Seguridad	
Jefa de la Sección de Protección de Datos	

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 Tratamiento de la UNED** son las personas físicas o jurídicas que determinan los fines y medios 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.

Boletín Interno de Coordinación Informativa

bici

Curso 2010/2011 21 - marzo - 2011 Número 23/Anexo I

ANEXO 4.9.

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)

http://www.uned.es
C/ Bravo Murillo,38
Tlfno. 91 398 6023
E-mail: bici@adm.uned.es

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.

Capitulo 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 decimoprimero 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. 16º.- 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. 17º.- 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. 18º.- Confidencialidad.

Las actuaciones realizadas por el Servicio de Inspección en el ejercicio de sus funciones, incluyendo la documentación obrante en los expedientes, informes o propuestas, 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 DE ENCARGO DE TRATAMIENTO

Estipulaciones

PRIMERA.- *Objeto del tratamiento*

Mediante las presentes cláusulas se habilita al ENCARGADO del tratamiento, para tratar por cuenta del RESPONSABLE de tratamiento, los datos de carácter personal necesarios para prestar el siguiente servicio:

_____

_____

La naturaleza y finalidad que justifican el tratamiento de los datos de carácter personal por cuenta del RESPONSABLE, son exclusivamente las que se indican en el Anexo I.

SEGUNDA.- *Devolución de los datos*

Una vez que finalice el presente acuerdo, el ENCARGADO devolverá al RESPONSABLE o en su caso, destruirá, los datos de carácter personal y, si procede, los soportes donde consten, una vez acabada la prestación. El retorno ha de comportar el borrado total de los datos existentes en los sistemas y documentos del ENCARGADO. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades por la ejecución de la prestación.

TERCERA.- *Obligaciones del ENCARGADO*

Finalidad: El ENCARGADO utilizará los datos personales sólo para la finalidad objeto de este tratamiento. En ningún caso podrá utilizar los datos para fines propios.

Subcontratación

El ENCARGADO no podrá subcontratar, ni total ni parcialmente, ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales sin autorización previa y por escrito del RESPONSABLE.

Si fuera necesario subcontratar, total o parcialmente, algún tratamiento de datos, este hecho se deberá comunicar previamente y por escrito al RESPONSABLE, con antelación suficiente, indicando los aspectos que se pretenden subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación deberá ser autorizada por escrito por el RESPONSABLE, siempre antes de su inicio y deberá regirse con lo estipulado en el artículo 28.4.del RGPD.

Instrucciones del RESPONSABLE: El ENCARGADO tratará los datos personales únicamente siguiendo instrucciones documentadas del RESPONSABLE.

Transferencia internacional: Si el ENCARGADO debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará por escrito al RESPONSABLE de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

Confidencialidad: El ENCARGADO y todo su personal mantendrán el deber de secreto respecto a los datos de carácter personal a los que hayan tenido acceso en virtud del presente encargo, incluso después de que finalice el mismo.

El ENCARGADO garantizará que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

Si existe una obligación de confidencialidad estatutaria deberá quedar constancia expresa de la naturaleza y extensión de esta obligación

El ENCARGADO mantendrá a disposición del RESPONSABLE la documentación acreditativa del cumplimiento de esta obligación.

Medidas de seguridad: El ENCARGADO con carácter periódico (y también siempre que haya cambios relevantes en su infraestructura de software y hardware) realizará una evaluación de riesgos en materia de seguridad de la información, de la que se derivarán la implantación de mecanismos adecuados a los riesgos detectados tal y como se describe en el artículo 32 del RGPD y en el Esquema Nacional de Seguridad y en concreto:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

La evaluación de riesgos de seguridad de la información deberá ser recogida en un informe por el ENCARGADO, que deberá proporcionarlo al RESPONSABLE. El alcance de dicha evaluación de riesgos de seguridad de la información será la totalidad de datos tratados por cuenta del RESPONSABLE. Las medidas de seguridad abarcarán la protección de los sistemas de información, así como de los sistemas de tratamiento manual y archivo de la documentación.

Registro de actividades de tratamiento: El ENCARGADO llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del RESPONSABLE con el contenido estipulado en el artículo 30.2 del RGPD, salvo que pueda ampararse en alguna de las excepciones del artículo 30.5 .

No comunicación: El ENCARGADO no comunicará los datos a terceras personas, salvo que cuente con la autorización expresa del RESPONSABLE, en los supuestos legalmente admisibles.

Formación de las personas autorizadas: El ENCARGADO garantizará la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

Ejercicio de los derechos: El ENCARGADO asistirá al RESPONSABLE, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados (acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de datos).

Notificación de violaciones de la seguridad: El ENCARGADO notificará al RESPONSABLE, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante consignada en el artículo 33.3. del RGPD.

Apoyo en realización de evaluaciones de impacto para la protección de datos: El ENCARGADO dará apoyo al RESPONSABLE en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

Cumplimiento de las obligaciones: El ENCARGADO pondrá a disposición del RESPONSABLE toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el RESPONSABLE u otro auditor autorizado por él.

Delegado de protección de datos: El ENCARGADO designará, si procede, un delegado de protección de datos y comunicará su identidad y datos de contacto al RESPONSABLE.

Firmado,

RESPONSABLE del tratamiento ENCARGADO del tratamiento

ANEXO I

FINALIDADES QUE JUSTIFICAN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR PARTE DEL ENCARGADO DE TRATAMIENTO

1. INTRODUCCIÓN

El presente Anexo forma parte del contrato de encargo de tratamiento suscrito entre las partes y detalla los aspectos y la identificación de la información afectada a los que accede o trata el Encargado de Tratamiento, la tipología de datos y las finalidades que justifican el tratamiento.

2. EL TRATAMIENTO DE DATOS PERSONALES INCLUIRÁ LOS SIGUIENTES ASPECTOS

(eliminar lo que no proceda):

- Recogida
- Registro
- Modificación
- Destrucción
- Conservación
- Comunicación
- Extracción
- Limitación
- Supresión
- Difusión
- Consulta

Otros: _____

3. IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE del tratamiento autoriza al ENCARGADO del tratamiento a tratar la información necesaria, lo que incluye las siguientes categorías de datos (eliminar lo que no proceda):

Datos identificativos: [Nombre y Apellidos, DNI, Nº SS, Dirección, Teléfono, Firma/Huella, Imagen/Voz]

Datos de naturaleza penal

Datos de infracciones y sanciones administrativas

Datos categorías especiales: [Salud, Datos genéticos o biométricos, 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 de circunstancias sociales: [Aficiones y estilo de vida; Pertenencia a clubes, asociaciones]

Datos académicos y profesionales: [Formación; Titulaciones; Expediente Académico; 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 transacciones: [bienes y servicios suministrados por el afectado; bienes y servicios recibidos por el afectado; transacciones financieras; compensaciones/indemnizaciones]

4. **FINALIDADES QUE JUSTIFICAN EL ACCESO O TRATAMIENTO POR PARTE DEL ENCARGADO**

   El Responsable del Tratamiento autoriza al Encargado de Tratamiento a tratar información de carácter personal de su titularidad, única y exclusivamente, para

   _____

   _____

En Representación de la UNED, En Representación de

ANEXO 5.2.

CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES

En _____ a _____ de _____ de 20___

Reunidos

De una parte, D _____, con DNI _____, en nombre y representación de _____ con domicilio en _____ y CIF _____, en adelante El RESPONSABLE del tratamiento.

Y de otra parte, D _____, con DNI _____, en nombre y representación propios / de _____ con domicilio en _____ y NIF/CIF _____, en adelante El ENCARGADO del tratamiento.

Ambas partes se reconocen mutuamente la capacidad legal bastante para suscribir este contrato y quedar obligadas en la representación en que respectivamente actúan. A tal fin,

Exponen

Que el Reglamento General de Protección de Datos (Reglamento UE 2016/679 del Parlamento Europeo y el Consejo) en adelante RGPD-UE, establece que el tratamiento de datos personales por parte de un encargado se regirá por un contrato u otro acto jurídico. El contenido de dicho contrato se regula en el artículo 28.3 del RGPD-UE

Estipulaciones

PRIMERA.- *Objeto del tratamiento*

Mediante las presentes cláusulas se habilita al ENCARGADO del tratamiento, para tratar por cuenta del RESPONSABLE de tratamiento, los datos de carácter personal necesarios para prestar el siguiente servicio:

_____

_____

La naturaleza y finalidad que justifican el tratamiento de los datos de carácter personal por cuenta del RESPONSABLE, son exclusivamente las que se indican en el Anexo al presente contrato.

SEGUNDA.- *Duración*

El presente acuerdo entrará en vigor a la fecha de su firma y permanecerá vigente mientras dure la prestación de servicios que motiva la formalización del presente contrato.

TERCERA.- *Devolución de los datos*

Una vez que finalice el presente acuerdo, el ENCARGADO devolverá al RESPONSABLE o en su caso, destruirá, los datos de carácter personal y, si procede, los soportes donde consten, una vez acabada la prestación. El retorno ha de comportar el borrado total de los datos existentes en los sistemas y documentos del ENCARGADO. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades por la ejecución de la prestación.

CUARTA.- *Obligaciones del ENCARGADO*

Finalidad: El ENCARGADO utilizará los datos personales sólo para la finalidad objeto de este tratamiento. En ningún caso podrá utilizar los datos para fines propios.

Subcontratación: El ENCARGADO no podrá subcontratar, ni total ni parcialmente, ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales sin autorización previa y por escrito del RESPONSABLE.

Si fuera necesario subcontratar, total o parcialmente, algún tratamiento de datos, este hecho se deberá comunicar previamente y por escrito al RESPONSABLE, con antelación suficiente, indicando los aspectos que se pretenden subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación deberá ser autorizada por escrito por el RESPONSABLE, siempre antes de su inicio y deberá regirse con lo estipulado en el artículo 28.4.del RGPD.

Instrucciones del RESPONSABLE: El ENCARGADO tratará los datos personales únicamente siguiendo instrucciones documentadas del RESPONSABLE.

Transferencia internacional: Si el ENCARGADO debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará por escrito al RESPONSABLE de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

Confidencialidad: El ENCARGADO y todo su personal mantendrán el deber de secreto respecto a los datos de carácter personal a los que hayan tenido acceso en virtud del presente encargo, incluso después de que finalice el mismo.

El ENCARGADO garantizará que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

Si existe una obligación de confidencialidad estatutaria deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.

El ENCARGADO mantendrá a disposición del RESPONSABLE la documentación acreditativa del cumplimiento de esta obligación.

Medidas de seguridad: El ENCARGADO con carácter periódico (y también siempre que haya cambios relevantes en su infraestructura de software y hardware) realizará una evaluación de riesgos en materia de seguridad de la información, de la que se derivarán la implantación de mecanismos adecuados a los riesgos detectados tal y como se describe en el artículo 32 del RGPD y en el Esquema Nacional de Seguridad y en concreto:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

La evaluación de riesgos de seguridad de la información deberá ser recogida en un informe por el ENCARGADO, que deberá proporcionarlo al RESPONSABLE. El alcance de dicha evaluación de riesgos de seguridad de la información será la totalidad de datos tratados por cuenta del RESPONSABLE. Las medidas de seguridad abarcarán la protección de los sistemas de información, así como de los sistemas de tratamiento manual y archivo de la documentación.

Registro de actividades de tratamiento: El ENCARGADO llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del RESPONSABLE con el contenido estipulado en el artículo 30.2 del RGPD, salvo que pueda ampararse en alguna de las excepciones del artículo 30.5 .

No comunicación: El ENCARGADO no comunicará los datos a terceras personas, salvo que cuente con la autorización expresa del RESPONSABLE, en los supuestos legalmente admisibles.

Formación de las personas autorizadas: El ENCARGADO garantizará la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

Ejercicio de los derechos: El ENCARGADO asistirá al RESPONSABLE, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados (acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos).

Notificación de violaciones de la seguridad: El ENCARGADO notificará al RESPONSABLE, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante consignada en el artículo 33.3. del RGPD.

Apoyo en realización de evaluaciones de impacto para la protección de datos: El ENCARGADO dará apoyo al RESPONSABLE en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

Cumplimiento de las obligaciones: El ENCARGADO pondrá a disposición del RESPONSABLE toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el RESPONSABLE u otro auditor autorizado por él.

Delegado de protección de datos: El ENCARGADO designará, si procede, un delegado de protección de datos y comunicará su identidad y datos de contacto al RESPONSABLE.

QUINTA.- *Obligaciones del RESPONSABLE*

Corresponde al RESPONSABLE del tratamiento:

a) Entregar al ENCARGADO los datos necesarios para la prestación de servicios a los que se refiere este acuerdo.

b) Realizar cuando así lo exija la normativa una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el ENCARGADO.

c) Realizar las consultas previas que corresponda ante las Autoridades de Protección de Datos.

d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD-UE por parte del ENCARGADO.

e) Supervisar el tratamiento de los datos, incluida la realización de inspecciones y auditorías.

SEXTA.- *Incumplimiento*

El incumplimiento por parte del ENCARGADO de las obligaciones referidas en el presente acuerdo comportará que sea considerado también responsable del tratamiento, respondiendo ante las Autoridades de Protección de Datos, o ante cualquier tercera persona de las infracciones que se puedan haber cometido derivadas de la ejecución del presente acuerdo o del cumplimiento de la legislación vigente en materia de protección de datos de carácter personal.

SÉPTIMA.- *Responsabilidad*

Tanto el RESPONSABLE como el ENCARGADO responderán de la totalidad de los daños y perjuicios que se irroguen a la otra parte en todos los supuestos de conducta negligente o culposa en el cumplimiento de las obligaciones que respectivamente les incumben, a tenor de lo pactado en el presente acuerdo.

Ninguna de las partes asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud del presente acuerdo si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor o caso fortuito admitido como tal por la Jurisprudencia, en particular: los desastres naturales, la

guerra, el estado de sitio, las alteraciones de orden público, la huelga en los transportes, el corte de suministro eléctrico o cualquier otra medida excepcional adoptada por las autoridades administrativas o gubernamentales.

OCTAVA.- *Notificaciones*

Toda notificación necesaria a los efectos del presente acuerdo se hará por escrito a la atención y dirección de quien consta en el encabezamiento del presente acuerdo.

NOVENA.- *Generalidades*

1. Este contrato contiene el total acuerdo entre las partes sobre el mismo objeto y sustituye y reemplaza a cualquier acuerdo anterior, verbal o escrito, al que hubieran llegado las partes.

   Asimismo, en caso de contradicción entre las condiciones estipuladas en el presente acuerdo y cualquier otro firmado con anterioridad entre ambas partes, prevalecerá lo estipulado en el presente acuerdo.

2. Cualquier modificación del contenido de este acuerdo, sólo será efectiva si se realiza por escrito y con el consentimiento de ambas partes.

3. La no exigencia por cualquiera de las partes de cualquiera de sus derechos de conformidad con el presente acuerdo no se considerará que constituya una renuncia de dichos derechos en el futuro.

DÉCIMA.- *Legislación y jurisdicción*

El presente acuerdo se regirá e interpretará conforme a la legislación española en todo aquello que no esté expresamente regulado, sometiéndose las partes, para las controversias que pudieran surgir en relación al mismo, a la competencia de los Juzgados y Tribunales de la ciudad señalada en el encabezamiento, con renuncia a cualquier otro fuero que les pudiera corresponder.

Firmado,

RESPONSABLE del tratamiento ENCARGADO del tratamiento

ANEXO I

FINALIDADES QUE JUSTIFICAN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR PARTE DEL ENCARGADO DE TRATAMIENTO

1. INTRODUCCIÓN

El presente Anexo forma parte del contrato de encargo de tratamiento suscrito entre las partes y detalla los aspectos y la identificación de la información afectada a los que accede o trata el Encargado de Tratamiento, la tipología de datos y las finalidades que justifican el tratamiento.

2. EL TRATAMIENTO DE DATOS PERSONALES INCLUIRÁ LOS SIGUIENTES ASPECTOS

(eliminar lo que no proceda)

- Recogida
- Registro
- Modificación
- Destrucción
- Conservación
- Comunicación
- Extracción
- Limitación
- Supresión
- Difusión
- Consulta

Otros: _____

3. IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE del tratamiento autoriza al ENCARGADO del tratamiento a tratar la información necesaria, lo que incluye las siguientes categorías de datos (eliminar lo que no proceda):

Datos identificativos: Nombre y Apellidos, DNI, Nº SS, Dirección, Teléfono, Firma/Huella, Imagen/Voz

Datos de naturaleza penal

Datos de infracciones y sanciones administrativas

Datos categorías especiales: Salud, Datos genéticos o biométricos, 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 de circunstancias sociales: Aficiones y estilo de vida; Pertenencia a clubes, asociaciones

Datos académicos y profesionales: Formación; Titulaciones; Expediente Académico; 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 transacciones: bienes y servicios suministrados por el afectado; bienes y servicios recibidos por el afectado; transacciones financieras; compensaciones/indemnizaciones

4. FINALIDADES QUE JUSTIFICAN EL ACCESO O TRATAMIENTO POR PARTE DEL ENCARGADO

El Responsable del Tratamiento autoriza al Encargado de Tratamiento a tratar información de carácter personal de su titularidad, única y exclusivamente, para

_____

_____

En Representación de la UNED,

En Representación de

ANEXO 5.3.

COMPROMISO DE GUARDAR SECRETO PROFESIONAL Y PROHIBICIÓN DE ACCESO A DATOS

_____[incluir la denominación social, o, en su caso, nombre y apellidos_____ **** [incluir la clase de servicios que presta] a _____ se compromete a que el personal designado para la prestación del/los citado/s servicio/s cumpla con las siguientes:

OBLIGACIONES

PRIMERA.- *Prohibición de acceder a los datos de carácter personal*

El personal de _____ [incluir la denominación social, o, en su caso, nombre y apellidos del tercero prestador de servicios], tiene prohibido, terminantemente, el acceso a los datos personales, contenidos en los diferentes soportes, informáticos o en papel, así como en los recursos del sistema de información, para la realización del trabajo encomendado.

SEGUNDA.- *Deber de secreto profesional*

Si por motivo de la realización del trabajo, 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 _____, tendrá la obligación de guardar secreto profesional respecto a la información accedida, aun después de haber cesado su relación laboral con ***** [incluir la denominación social, o, en su caso, nombre y apellidos del tercero prestador de servicios]. En este sentido _____ [incluir la denominación social, o, en su caso, nombre y apellidos del tercero prestador de servicios] se compromete a firmar con sus empleados los correspondientes compromisos de confidencialidad. Para la comprobación de esta obligación por la UNED en cualquier momento podrá requerir certificados que justifiquen que los trabajadores que prestan servicios en las instalaciones de la UNED han formado los compromisos de confidencialidad.

Es obligación de este último, comunicar este deber a su personal, así como cuidar de su cumplimiento.

TERCERA.- *Responsabilidad*

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 utilizase para cualquier menester, será considerado como Responsable de Tratamiento. Así, responderá personalmente por las infracciones cometidas.

D/Dª Por la UNED	D/Dª Por EL PRESTADOR DE SERVICIOS

ANEXO 6.1.

ACTUALIZACIÓN SEMESTRAL, del 1 de ……. al 30 de …….. de 20.. DE LAS ACTIVIDADES Y TRATAMIENTO DE LOS 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 informativas 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.

FORMULARIO PARA LA CREACIÓN DE LA ACTIVIDAD DE TRATAMIENTO

1. - DATOS PRELIMINARES

Empresa

Nombre y Apellidos del colaborador/a

Área o Departamento

Cargo o puesto de trabajo

2.- NOMBRE DE LA ACTIVIDAD DE TRATAMIENTO

Sistema de tratamiento

☐ Automatizado [Informático]
☐ Cloud (Nube). Indicar la compañía que presta el servicio: _____
_____
☐ Manual [Papel]
☐ Mixto

En caso de realizar el tratamiento automatizado, indicar la aplicación informática empleada para tales efectos

☐ Excel
☐ Access
☐ Word
☐ Otros [indicar en el recuadro el nombre del programa o aplicación informática]

3.- ORIGEN O PROCEDENCIA DE LOS DATOS

☐ El propio interesado o su representante legal
☐ Otras personas físicas
☐ Fuentes accesibles al público [boletines o diarios oficiales; listas o guías de profesionales; medios de comunicación; guías o repertorios de telefonía]
☐ Registros públicos
☐ Administraciones Públicas

4.- TIPOLOGÍA DE DATOS DE CARÁCTER PERSONAL

Datos de carácter identificativo

☐ NIF/DNI
☐ Nombre y apellidos
☐ Dirección [Postal/Electrónica]
☐ Nº Registro de personal
☐ Tarjeta Sanitaria
☐ Firma electrónica
☐ Teléfono [Fijo/Móvil]
☐ Nº SS / Mutualidad
☐ Imagen / voz
☐ Firma

Otros datos de especial atención

☐ Datos de menores de 14 años
☐ Datos relativos a condenas e infracciones penales

Categorías especiales de datos

☐ Ideología u opiniones políticas
☐ Afiliación sindical
☐ Religión
☐ Convicciones religiosas o filosóficas
☐ Origen racial o étnico
☐ Salud [física o psíquica]
☐ Datos biométricos (huella dactilar, iris…)
☐ Datos genéticos
☐ Vida y/u orientación sexual
☐ Víctima de violencia de género

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; 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 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]

5.- PLAZO DE CONSERVACIÓN DE LOS DATOS

Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación.

En caso de tener un plazo específico definido, indicar cuál.

6.- TERCEROS AJENOS A LA ORGANIZACIÓN PRESTADORES DE SERVICIOS CON ACCESO A DATOS O ENCARGADOS DE TRATAMIENTO

☐ Asesoría [Contable, Fiscal y/o Laboral]
☐ Auditores [Contable o fiscal, Calidad, Medio Ambiente, Otros]
☐ Informática (suministro y/o mantenimiento de hardware y/o software)
☐ Alojamiento hosting o housing, cloud
☐ Marketing directo (Mailing)

OTROS SERVICIOS [Indicar en el recuadro]

7.- CESIÓN O COMUNICACIÓN DE DATOS

☐ Organismos de la Seguridad Social
☐ Administración Tributaria
☐ Registro públicos
☐ Órganos judiciales
☐ Otros órganos de la Administración Pública
☐ Sindicatos y juntas de personal
☐ Colegios profesionales
☐ Comisión Nacional del Mercado de Valores
☐ Notarios, Abogados, Procuradores
☐ Organismos de la Unión Europea
☐ Entidades dedicadas al cumplimiento/incumplimiento obligaciones dinerarias
☐ Organizaciones y asociaciones sin ánimo de lucro
☐ Empresas dedicadas a la publicidad o marketing directo
☐ Fuerzas y cuerpos de seguridad
☐ Bancos, Cajas de ahorro y cajas rurales
☐ Otras entidades financieras
☐ Entidades aseguradoras
☐ Entidades Sanitarias

OTROS DESTINATARIOS [Indicar en el recuadro]

8.- MOVIMIENTOS O TRANSFERENCIAS INTERNACIONALES.

¿Realiza o prevé realizar movimientos internacionales de datos dentro del Espacio Económico Europeo?

No ☐ **Sí** ☐ Señale el país destinatario

	Alemania		Francia		Polonia
	Austria		Grecia		Portugal
	Bélgica		Holanda		Reino Unido
	Bulgaria		Hungría		República Checa
	Chipre		Irlanda		República Eslovaca
	Croacia		Italia		Rumanía
	Dinamarca		Letonia		Suecia
	Eslovenia		Lituania		Finlandia
	Estonia		Luxemburgo		Malta

¿Realiza o prevé realizar transferencias internacionales de datos a terceros países fuera del Espacio Económico Europeo y/o, en su caso, organizaciones internacionales?

No ☐ **Sí** ☐

Una ***"transferencia internacional de datos",*** es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del Responsable del Tratamiento establecido en territorio español.

Se entenderá por ***"organización internacional"****:* la organización internacional y sus entes subordinados de Derecho internacional público u otros organismos creados por un acuerdo entre dos o más países o basados en él.

A continuación, señale si se trata de uno de los siguientes países destinatarios, los cuales son considerados con un nivel de protección equiparable a España.

	Islandia		Andorra
	Liechenstein		Uruguay
	Suiza		Nueva Zelanda
	Canadá		Isla de Man
	Argentina		Jersey
	Guernsey		Islas Feroe
	Israel		

En su caso, indique la Organización Internacional que pueda ser destinataria:

En caso de que la transferencia de los datos se realice a ESTADOS UNIDOS, indicar el Estado/s o ciudad/es donde se opera:

En el caso de que realice transferencia de datos personales a otros países distintos de todos los anteriores, indique, por favor, cuál:

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 del artículo 10 del 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, 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.

Formulario de presentación de quejas o sugerencias del Código de Conducta

Comunicación de quejas o sugerencias relativas a la aplicación del "Código de Conducta en materia de Protección de Datos de la Universidad Nacional de Educación a Distancia (UNED)"

Datos del solicitante:

D./Dª _____ mayor de edad, con domicilio en _____ nº _____ Localidad _____ Provincia _____ Código _____ teléfono _____ mail _____ con DNI nº _____ del que se acompaña fotocopia, por medio del presente formulario manifiesta su deseo de ejercer su derecho de presentación de quejas o sugerencias, 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 de Conducta 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
dptojuridicoseguridad@adm.uned.es

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

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.

jhermoso@pas.uned.es ext.: 6068 vmartin@pas.uned.es ext.: 7291

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

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.

ANEXO 10.3.

Estimado/a compañero/a:

Como Responsable de tratamiento de datos de carácter personal de la UNED, es importante que conozcas la actualización de la normativa vigente en materia de protección de datos.

El nuevo Reglamento General de Protección de Datos (RGPD) de la Unión Europea, publicado en mayo de 2016, será ***aplicable a partir del 25 de mayo de 2018***.

Dos elementos de carácter general constituyen la ***mayor innovación del RGPD*** para los responsables de los tratamientos y se proyectan sobre todas las obligaciones de las organizaciones:

El Principio de responsabilidad Proactiva: Que aplicado a los tratamientos requiere que las organizaciones analicen ***qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones*** frente a todos los tratamientos de datos personales que lleven a cabo.

El Enfoque de Riesgo: El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta ***la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas***.

Por todo ello, desde el Departamento hemos adaptado y actualizado la información contenida en la página Web de Protección de Datos de la UNED (será necesario estar autenticado para ver toda la información):

- Normativa vigente
- Cláusulas informativas, cuando se recogen datos personales (**es necesario actualizar los formularios** que contengan estas cláusulas)
- Ejercicio de los derechos en materia de protección de datos
- Contratos y cláusulas de encargados de tratamiento
- Procedimientos de gestión de tratamientos de datos personales
- Inventario de las actividades de los tratamientos
- El Código de Conducta de la UNED
- Oficina del Delegado de Protección de Datos

Asimismo, figura toda la información de interés relacionada con esta materia.

Se adjuntan documentos elaborados por la Agencia Española de Protección de Datos con las principales novedades.

Te ruego que hagas la **máxima difusión** entre el personal adscrito a tu unidad y te agradezco tu participación en la protección de datos personales en la Universidad.

Atentamente,

ANEXO 10.4.

COMUNICADO SOBRE LA UTILIZACIÓN DE BASES DE DATOS Y DERECHOS DE LOS ESTUDIANTES

Para general conocimiento, se remite información de interés sobre la utilización de las bases de datos de estudiantes no actualizadas, con el objetivo de no vulnerar la legislación sobre protección de datos de carácter personal en lo relativo a la creación y utilización de **Ficheros temporales** por personal de la Universidad.

Se han detectado casos de estudiantes que **siguen recibiendo** información de cursos, actividades organizadas por la UNED o de entidades directamente relacionadas con ésta, a pesar de que **no han autorizado en el proceso de matrícula,** la recepción de comunicaciones sobre publicidad de cursos, **o han ejercido el derecho de cancelación** de sus datos personales a estos efectos.

Por todo ello se han de tener en cuenta las normas siguientes:

- **Siempre** deberán utilizarse las bases de datos del proceso de matrícula, al estar actualizadas diariamente. De esta manera se cumple con el principio de *"Calidad de los datos", que establece que los datos deben ser exactos y actualizados.* En caso contrario se estaría incumpliendo la normativa sobre la materia.
- **Los Ficheros temporales deberán eliminarse en el plazo de un mes**, cuando hayan dejado de ser necesarios para los fines que motivaron su creación, como así lo señala la Normativa de seguridad y buen uso del Sistema de Información de la UNED.
- No tener en cuenta estas medidas, **puede constituir una falta grave** del usuario, según la citada normativa.

La Gerencia de la UNED,

ANEXO 10.5.

Estimado miembro de la comunidad universitaria:

Adjunto orientaciones de la Agencia Española de Protección de Datos para la aplicación provisional de la Disposición adicional séptima de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, **referente a la identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos:**

Orientaciones de la Agencia Española de Protección de Datos

Disposición adicional séptima. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

1. Cuando sea necesaria ***la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento*** *nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente****. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.***

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. ***En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.***

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Te ruego que hagas la **máxima difusión** entre el personal adscrito a tu unidad y te agradezco tu participación en la protección de datos personales en la Universidad.

Un saludo,

La Gerente de la UNED