Universidad Internacional de La Rioja (UNIR)

ESIT

Máster universitario en Seguridad Informática

Metodología para la aplicación de RGPD y LOPDGDD en proyectos de investigación universitaria.

Trabajo Fin de Máster

Presentado por: Gutiérrez Fuente, Roberto

Director: Delgado Sotés, Juan José

Ciudad: Valladolid
Fecha: 27 de febrero de 2020

Resumen

La reciente evolución de la normativa en la protección de datos de carácter personal ha afectado a todas aquellas áreas que trabajan con este tipo de información, incluida la investigación universitaria española.

En este trabajo, se plantea un análisis de dicha evolución normativa y los puntos clave que afectan a todos aquellos proyectos de investigación que incluyen datos personales. Derivada de este proceso, se propone una metodología que ayude a los investigadores a incorporar a la gestión administrativa de sus proyectos todas las posibles obligaciones en materia de protección de datos. Además, ayudará a que las distintas universidades responsables dispongan de toda la información necesaria sobre estos tratamientos.

El resultado es un modelo teórico verificado y considerado como útil por un conjunto de investigadores consultado.

Palabras Clave: Tratamiento de datos personales, investigación universitaria, RGPD.

Abstract

The recent evolution of General Data Protection Regulation has affected all those areas that work with this type of information, including Spanish university research.

The aim of this paper is to examine this regulatory evolution and the key points that affect all those research projects that include personal data. As a result of this process, the proposed methodology will help researchers to incorporate all possible data protection obligations into the administrative management of their projects. Furthermore, it will help to ensure that the different responsible universities have all the necessary information on these processes.

The result is a fully verified theoretical model, considered useful by a group of researchers consulted.

Keywords: Personal data treatment, university research, GDPR.

Índice de contenidos.

Índice de figuras.

Relación de acrónimos.

AEI	Agencia Estatal de Investigación
AEMPS	Agencia Española de Medicamentos y Productos Sanitarios
AEPD	Agencia Española de Protección de Datos
AMM	Asociación Médica Mundial
BOE	Boletín Oficial del Estado
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CE	Consejo de Europa
CE	Constitución Española
CEEA	Comité de Ética de Experimentación Animal
CEI	Comité de Ética de la Investigación
CEIC	Comité de Ética de la Investigación Clínica
CEIm	Comité de Ética de la Investigación con Medicamentos
CI	Consentimiento Informado
CRUE	Conferencia de Rectores de las Universidades Españolas
DLP	Data Loss Prevention
DNI	Documento Nacional de Identidad
DPD	Delegado de Protección de Datos
DPO	Data Protection Officer
EIPD	Evaluación de Impacto relativa a la Protección de Datos
GT29	Grupo de Trabajo del Artículo 29 o Grupo de la protección de las personas en lo que respecta al tratamiento de datos de carácter personal
HIP	Hoja de Información al Paciente
HMAC	Hash-based Message Authentication Code
I+D+i	Investigación, Desarrollo e Innovación
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission

IP	Internet Protocol
IP	Investigador Principal
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
LAP	Ley de Autonomía del Paciente
LCTI	Ley de la Ciencia, la Tecnología y la Innovación
LIB	Ley de Investigación Biomédica
LO	Ley Orgánica
LOPD	Ley Orgánica de Protección de Datos Personales
LOPDGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
LOU	Ley Orgánica de Universidades
LPHE	Ley del Patrimonio Histórico Español
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
NIF	Número de Identificación Fiscal
NSS	Número de la Seguridad Social
OCDE	Organización para la Cooperación y el Desarrollo Económico
PAS	Personal de Administración y Servicios
PDI	Personal Docente e Investigador
PEI	Personal Empleado Investigador
PIA	Privacy Impact Assessment
RAE	Real Academia Española
RAT	Registro de Actividades de Tratamiento
RDECM	Real Decreto por el que se regulan los Ensayos Clínicos con Medicamentos, los Comités de Ética de la Investigación con Medicamentos y el Registro Español de Estudios Clínicos
RGPD	Reglamento General de Protección de Datos
SECTI	Sistema Español de Ciencia, Tecnología e Innovación

TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la Información y la Comunicación
UE	Unión Europea

1. Introducción.

La *Comunidad Europea* ha vivido recientemente un proceso de renovación de sus principales normas en materia de protección de datos de carácter personal. Este proceso ha culminado con la publicación 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 esos datos y por el que se deroga la Directiva 95/46/CE* (*Reglamento General de Protección de Datos*, en adelante, *RGPD*).

En España, esta transformación se ha visto complementada con la publicación de la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (en adelante, LOPDGDD).

Este conjunto de publicaciones proporciona un entorno legal y de procedimientos que, si bien mantiene muchas de las bases o filosofía de la normativa anterior, genera un nuevo conjunto de derechos y obligaciones en torno al tratamiento de los datos personales y obliga a todas aquellas entidades que trabajen con este tipo de datos a ejecutar la correspondiente revisión y adaptación.

Uno de los campos afectados por este cambio es el mundo de la investigación universitaria, ya que se trata de un gran consumidor de datos de carácter personal (al menos, en determinados proyectos, como los de investigación médica) y no puede eludir esta evolución normativa. Todos sus procedimientos y protocolos (en aquellos casos en que estén establecidos) deben alinearse con las nuevas exigencias regulatorias.

1.1. Motivación y enfoque.

Tras la reciente publicación de las mencionadas normas, las universidades españolas han comenzado una fase de revisión de procedimientos y reglamentos internos para adaptarse al nuevo entorno.

Una de las consecuencias de este proceso es la reciente creación, por parte de *CRUE Universidades Españolas*, de un grupo de trabajo, llamado *Delegados de Protección de Datos* (encajado en la comisión sectorial *Secretarías Generales*). Este grupo ha comenzado a organizar ciertos trabajos y reuniones, relacionados con la gestión de los datos personales en la comunidad universitaria.

Pero el campo concreto de la gestión de los tratamientos de datos de carácter personal en el ámbito de la investigación universitaria sigue adoleciendo de una falta de protocolización específica (al menos, si existe en alguna universidad, no está accesible al público general).

Por lo tanto, se detecta un vacío de procedimientos común, y este hecho es parte del problema que se tratará en este trabajo.

Por otro lado, en muchos casos (sobre todo en universidades medianas-pequeñas), la gestión administrativa de los proyectos recae en los propios investigadores que, en muchas ocasiones, carecen de la formación necesaria para tratar adecuadamente todos los requisitos de seguridad que debieran ser aplicados a los tratamientos de datos de carácter personal. Esto representa un serio riesgo para los intereses de los titulares de dichos datos, por lo que es fundamental aplicar medidas que ayuden a reducirlo, ya que las sanciones previstas por la nueva normativa y aplicadas por la *Agencia Española de Protección de Datos* (en adelante, AEPD) pueden llegar a ser realmente importantes.

1.2. Objetivos y planteamiento del trabajo.

Una vez presentada la problemática en torno a la gestión de los datos de carácter personal en el ámbito de la investigación universitaria, procede presentar los objetivos generales de este trabajo.

El objetivo fundamental es elaborar una metodología que permita estandarizar (y así facilitar o simplificar lo más posible) las tareas administrativas y de gestión relacionadas con los datos de carácter personal incluidos en los proyectos de investigación universitaria. El uso de dicha herramienta (compuesta por un conjunto de protocolos, procedimientos, manuales y plantillas) deberá permitir a los investigadores aplicar mucho más ágil y fácilmente las normativas, estándares y buenas prácticas en la materia de gestión de datos personales, sean o no expertos en la misma, y garantizar que los tratamientos aplicados lo sean con el menor riesgo posible para los interesados o propietarios de dichos datos.

La aportación se orienta, sobre todo, a pequeños equipos de investigación ubicados en el ámbito de universidades privadas de tamaño medio/pequeño; ya que en esos entornos los recursos suelen estar limitados y puede ser más necesaria cualquier tipo de ayuda.

Para la consecución de dicho objetivo, se plantea la realización de las siguientes tareas (cuyos resultados conforman la base de construcción de la metodología propuesta):

1. Análisis de las normas mencionadas sobre protección de datos, junto con las específicas del ámbito de la investigación (Ej.: Ley de la Ciencia, la Tecnología y la Innovación; Ley de investigación Biomédica Española, etc.) y otra información relacionada (por ejemplo, informes y guías de la *Agencia Española de Protección de Datos*) y extracción de todas las consideraciones que pudieran afectar al objeto del estudio.

2. Diseño de una plantilla para que el investigador, en el caso de producirse un tratamiento de datos de carácter personal en su proyecto, pueda identificar correctamente la correspondiente actividad y todos sus parámetros. Esta es la información que deberá comunicar al Delegado de Protección de Datos o responsable equivalente de la universidad, con el objetivo de que éste pueda mantener el *Registro de Actividades de Tratamiento* actualizado (procedimiento obligatorio según las nuevas normativas).
3. Diseño de un modelo que permita:
    a. Identificar los riesgos clave asociados a este tipo de tratamientos.
    b. Clasificar los proyectos de investigación en función del riesgo con respecto al tratamiento datos personales.
4. Diseño de plantillas para generar la documentación relacionada con protección de datos, principalmente:
    a. Sistema de consentimientos.
    b. Clausulado en formularios.
5. Elaboración de un catálogo de modos de anonimización y seudonimización seguros de datos para aplicar en este tipo de proyectos.
6. Elaboración de un catálogo de modos en los que implementar el acceso a sus derechos por parte de los interesados.
7. Diseño de un catálogo de medidas de seguridad a aplicar por los investigadores y por la universidad, en función del tipo de proyecto identificado. Para ello, se analizarán los estándares existentes.
8. Extracción de las implicaciones que, para la ejecución de los distintos tipos de tratamientos identificados, deberían suministrarse a la dirección de la universidad para ser incorporadas al *Programa de Cumplimiento de Protección de Datos* de la misma.
9. Integrar los resultados obtenidos de las anteriores tareas en una metodología y evaluar los resultados de su aplicación.

1.3. Estructura del documento.

La estructura de este trabajo es la siguiente:

En el presente **Capítulo 1**, se resumen el problema a tratar, los objetivos del trabajo y el modo de plantearlo y organizarlo.

En el **Capítulo 2**, se resume la situación actual en lo que se refiere al estado del arte relativo a los procedimientos y normativas relacionados con la protección de datos de carácter personal. Se analiza la normativa vigente, comenzando desde el plano general y descendiendo hacia la realidad de la investigación universitaria.

En el **Capítulo 3**, se presentan los objetivos (general y específicos) y se describen las fases que componen la metodología de trabajo seguida en este proyecto.

En el **Capítulo 4**, se desarrolla la contribución específica aportada por el proyecto. En primer lugar, se identifican tres requisitos: legales, organizativos y de formación. Posteriormente, se describe la metodología objeto de esta memoria, revisando las fases que la componen. Finalmente, se describe el método de validación de dicha metodología.

Por último, en el **Capítulo 5**, se recogen las conclusiones del estudio y una relación de posibles líneas futuras de trabajo.

2. Contexto y estado del arte.

2.1. Conceptos clave.

En la presente memoria se utilizan muchos conceptos específicos del área de la protección de datos personales y del entorno de la investigación universitaria. Algunos de ellos, se presentan a continuación.

- **Dato de carácter personal.**

Ampliando la definición que aporta la AEPD en su guía *Protección de datos: Guía para el Ciudadano*, los datos de carácter personal son cualquier información (numérica, alfabética, gráfica, fotográfica, acústica, biométrica, o de cualquier otro tipo) referente a personas físicas identificadas o identificables ('interesados'), de forma que puede ser identificable toda persona cuya identidad pueda determinarse mediante un identificador (por ejemplo, un nombre, un número de identificación, datos de localización o un identificador en línea) o mediante el uso de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de las personas (Agencia Española de Protección de Datos, 2018).

Se pueden establecer distintas clasificaciones sobre los datos de carácter personal:

- *Datos identificativos*. Nombre y apellidos, NIF/DNI, pasaporte o similar, dirección postal, dirección de correo electrónico, imagen, voz, NSS, teléfono, huella dactilar, firma electrónica, dirección IP, etc. Este conjunto de datos es fundamental, ya que es el que permite identificar al individuo y asociar con él el resto de la información.
- *Datos especialmente protegidos*. Ideología, opiniones políticas, afiliación sindical, creencias, religión, origen racial o étnico, datos médicos o de salud y vida sexual, así como el tratamiento de los datos genéticos y biométricos (si identifican a la persona de manera unívoca).
- *Datos relativos a características personales*. Estado civil, datos de familia, fecha nacimiento, lugar nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas, información genética, etc.
- *Datos relativos a circunstancias sociales*. Características de alojamiento, vivienda, situación familiar, propiedades, aficiones, estilos de vida, licencias, etc.
- *Datos académicos y profesionales*. Datos de currículo, expediente académico, titulaciones, etc.
- *Datos sobre empleo*. Profesión, puesto de trabajo ocupado, datos de la nómina, historial del trabajador, etc.

- *Datos que aportan información comercial*.
- *Datos económicos, financieros y de seguros*.
- *Datos relativos a condenas, multas e infracciones penales*.
- *Etc.*

De relevancia fundamental para este estudio serán los datos especialmente protegidos relativos a la salud, genéticos y biométricos; ya que son habitualmente utilizados en muchos proyectos de investigación.

- **Privacidad y protección de datos.**

Los conceptos de privacidad y protección de datos, aunque cercanos, no son exactamente sinónimos. La privacidad hace referencia de forma general a la protección de la esfera privada de las personas, es un concepto más general y recogido habitualmente por las normas de primer orden jerárquico. Por otro lado, la protección de datos incide, de forma más específica, en el modo en que se aseguran los procesos de tratamiento de datos relativos a un individuo identificado o identificable.

- **Tratamiento de datos.**

La *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (LOPD) definió “tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias” (art. 3 LO 15/1999, de 13 de diciembre). En la nueva ley, no hay referencias o menciones para re-definir este concepto.

Por su parte, el RGPD define tratamiento como (art. 4 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril):

> 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,

definición muy similar a la que, en su día, propuso la Directiva 95/16/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- **Responsable del tratamiento.**

La LOPD definió “Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento” (art. 3 LO 15/1999, de 13 de diciembre). En la nueva ley, no hay referencias o menciones para re-definir este concepto. Es importante mencionar que el concepto de ‘fichero’ hace referencia, en esta ley, a “todo conjunto organizado de datos de carácter personal que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso” (art. 3 LO 15/1999, de 13 de diciembre).

Por su parte, el RGPD, matiza la definición de responsable como (art. 4 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril):

> 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.

En este caso, lo importante de la definición es determinar quién toma las decisiones, es decir, el responsable será quien decida para qué se van a utilizar los datos y qué medios se van a emplear para hacerlo. Es fundamental identificar al responsable o responsables de cada tratamiento.

- **Encargado del tratamiento.**

La LOPD definió “Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento” (art. 3 LO 15/1999, de 13 de diciembre). En la nueva ley, no hay referencias o menciones para re-definir este concepto.

La definición aportada por el RGPD, es muy similar.

- **Legitimación para poder aplicar un tratamiento de datos.**

La protección de sus datos de carácter personal es un derecho de los ciudadanos y, por lo tanto, para que cualquier entidad pueda tratarlos es necesario que cuente con la correspondiente legitimación. Es decir, siempre que se produzca un tratamiento de datos de carácter personal, deben existir bases jurídicas que permitan, legitimen u otorguen validez legal a dicho tratamiento. Como se verá más adelante, dichas bases jurídicas están

perfectamente definidas y acotadas en las normativas vigentes, y será fundamental identificar las adecuadas en cada caso.

- **Cesión o comunicación de datos y acceso a datos.**

Una cesión o comunicación de datos se produce cuando el responsable de un tratamiento de datos de carácter personal entrega dichos datos a un tercero. El que los recibe, podrá decidir sobre sobre el uso y finalidades a aplicar sobre ellos, es decir, será un nuevo responsable del tratamiento.

Por el contrario, el acceso a datos se produce cuando un tercero (normalmente un encargado del tratamiento) accede a dichos datos para prestar un servicio al responsable de los mismos. En este caso, el encargado no podrá decidir sobre los usos o finalidades del tratamiento.

- **Autoridades de control.**

El concepto de Autoridad de control se introdujo con el denominado *Convenio 108* (Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, 1981). Por su parte, la primera directiva europea que abordó en profundidad la protección de datos personales, la Directiva 95/16/CE, en su capítulo VI, estableció nuevas normativas sobre estas entidades. Se trata de una o más autoridades públicas, dispuestas por los Estados miembros, cuya misión es vigilar la aplicación -en sus respectivos territorios- de las disposiciones adoptadas por ellos. Este concepto ha perdurado y se ha reforzado en las sucesivas normativas promulgadas, siendo hoy día un elemento fundamental para la protección de datos de carácter personal. En el caso español, la autoridad principal es la *Agencia Española de Protección de Datos* (AEPD), fundada en 1992, y actualmente también existen agencias de carácter autonómico en Cataluña, País Vasco y Andalucía.

- **Seudonimización y anonimización.**

El RGPD define *seudonimización* como (art. 4 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril)

> el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Por su parte, la *anonimización* o *disociación* de los datos personales va más allá y supone la ruptura total entre los datos personales y los datos identificativos de las personas afectadas, de forma que no se puedan volver a asociar de ningún modo (así se definía en la antigua

LOPD). Este proceso supone que el tratamiento de datos anonimizados deja de ser un tratamiento de datos de carácter personal (por este motivo, ni el RGPD ni la LOPDGDD definen anonimización ni la incluyen como medida de seguridad dentro de los tratamientos de datos personales).

En muchos casos, la anonimización o disociación puede ser el proceso fundamental que habilite la utilización segura de algunos datos de tipo personal en investigación.

- **Investigación universitaria.**

Según la RAE, la acepción de *investigar* aplicable en el contexto de este trabajo es "realizar actividades intelectuales y experimentales de modo sistemático con el propósito de aumentar los conocimientos sobre una determinada materia" (Real Academia Española, 2014).

El entorno universitario es uno de los más propicios para llevar a cabo esta actividad. Como explica Posas (2018), las universidades juegan un papel fundamental en la sociedad actual, ya que –al menos las universidades más importantes- destacan no sólo por su facultad de transmitir los conocimientos, sino también por su enorme capacidad de generarlos. Actualmente, un porcentaje muy elevado de la investigación en España se lleva a cabo en las universidades y, dejando aparte los posibles problemas relacionados con la financiación de esta actividad en épocas de crisis, este papel se mantendrá en un futuro.

- **Grupo de investigación.**

Se trata de la unidad básica en la que se organizan los investigadores. La definición es sencilla: se trata de un conjunto de personas que investigan juntas. Pueden ser grupos más o menos grandes, más o menos activos, más o menos locales o globales y más o menos oficiales (dependiendo del grado de reconocimiento obtenido en las diferentes entidades en las que participan). Sirven para organizar y maximizar la capacidad de trabajo de sus componentes, así como para poder reunir un mayor número de méritos académicos y acceder a los proyectos ofertados. ´

En este contexto, es importante hablar también de los llamados *Investigadores Principales* (IP). Se trata de cada una de las personas que están a cargo de un proyecto, normalmente asociado a una subvención para investigación (son titulares de la misma). Habitualmente son sus nombres los que figuran en los procesos administrativos asociados a dichos proyectos, junto con el de las universidades y otras entidades implicadas.

- **Comités de Ética de la Investigación.**

Se trata de órganos colegiados constituidos para garantizar “la adecuación de los aspectos metodológicos, éticos y jurídicos” en dichos procesos de investigación, sobre todo cuando éstos incluyen “intervenciones en seres humanos o la utilización de muestras biológicas de origen humano” (preámbulo II Ley 14/2007, de 3 de julio). Todos aquellos proyectos de investigación que requieran la realización de actividades como las indicadas, deberán contar con informe previo favorable del correspondiente *Comité de Ética de la Investigación* (CEI). Como se verá más adelante, existen otros comités de ética especializados, aparte de los CEI.

2.2. Marco normativo.

No se puede comenzar a revisar las materias sobre las que trata este estudio sin antes estudiar el marco normativo, ya que es una referencia vinculante fundamental en el desarrollo de cualquier metodología que afecte al tratamiento de datos personales.

En este apartado, primero, se realiza un pequeño recorrido sobre la evolución de las principales normativas aplicables en materia de protección de datos y, posteriormente, se mencionan las principales leyes que regulan los procesos de investigación objeto del estudio.

2.2.1. Privacidad y protección de datos en el contexto internacional. Evolución.

Antes de nada, señalar que, al menos en el ámbito europeo, la privacidad y la protección de datos de carácter personal están consideradas como derechos fundamentales y, por lo tanto, han tenido un peso fundamental en la generación de las sucesivas normativas reguladoras.

Una de las primeras referencias a esta idea surge en 1950 con el *Convenio Europeo de Derechos Humanos* (Convenio para la protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente). Este convenio tuvo como objetivo proteger los derechos humanos y las libertades fundamentales de las personas pertenecientes a los estados miembros. Concretamente, su artículo 8 protege el derecho al respeto a la vida privada y familiar, y la jurisprudencia del *Tribunal Europeo de Derechos Humanos* ha entendido que, en el ámbito de este precepto, ha de entenderse incluido el derecho a la protección de los datos de carácter personal.

En 1957, el *Tratado de Funcionamiento de la Unión Europea* estableció que “toda persona ostenta el derecho a la protección de los datos de carácter personal que le conciernan” (art. 16 TFUE, Versión consolidada 2010). Este documento fue uno de los cuatro pilares de la constitución de lo que hoy se conoce como *Unión Europea*.

Unos años más tarde, en 1980, un importante foro internacional como la *Organización para la Cooperación y el Desarrollo Económicos* (OCDE) publicó un documento en el que recogía sus *Directrices de Privacidad* (Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, 1980). Este documento, aunque no vinculante, constituyó un importante hito, ya que –en el campo de la protección de los datos personales- comenzó a recoger principios como la limitación de recogida, calidad de los datos, especificación de los fines, limitación de uso, salvaguarda de la seguridad, transparencia, participación individual y responsabilidad. Además, esta misma organización, ha sido la primera en proponer la actualización de sus directrices, en 2013, con el objetivo de adaptarlas a la evolución tecnológica, social y económica.

Otro hecho relevante, dentro de este pequeño repaso histórico, es la adopción en 1981 (aunque no entró en vigor hasta 1985) por parte del *Consejo de Europa*, del llamado *Convenio 108* (Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, 1981). Esta normativa se convirtió en uno de los más importantes instrumentos internacionales vinculantes en esta materia, ratificado hoy día por más de 50 países (de dentro y fuera de la Unión Europea). Adoptarlo supone asumir importantes responsabilidades, compromisos y obligaciones con respecto a la protección de los datos personales. Se fijan unos principios básicos y unos requisitos que ayudan a determinar si un tratamiento se ajusta a la ley y se establecen una serie de derechos respecto a las personas titulares de dichos datos. También se incluye una especial atención a la gestión de los considerados datos sensibles, como, por ejemplo, los de salud. En 2018 fue reformado y adaptado a las nuevas normativas, generando lo que se conoce como el *Convenio 108+* (Convention for the protection of individuals with regard to the processig of personal data. Convention 108+, 2018). Este convenio ha sido una herramienta fundamental en el campo y se pueden encontrar sus influencias en muchas de las normativas actualmente vigentes.

En 1995, se publica en la Unión Europea una normativa fundamental, la *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Una de las principales implicaciones de esta norma fue la ampliación del concepto de 'libre circulación entre los estados' a los datos personales. Esto fue debido a que, en los años previos a su promulgación, la generalización de tratamientos en muchos ámbitos de cooperación internacional (administrativa, científica, técnica, etc.) era cada vez más patente y las diferencias jurídicas entre estados no podía suponer un freno al flujo transfronterizo. Era necesaria una armonización de las legislaciones nacionales en este campo y esto se empezó a considerar como prioritario en las instituciones comunitarias. Esta directiva ha sido un texto fundamental de referencia en esta materia a escala europea y se

puede observar que algunos de los principios recogidos en la norma vienen a ampliar los recogidos previamente en el citado Convenio 108.

La Directiva 95/46/CE también propuso la creación del *Grupo de la protección de las personas en lo que respecta al tratamiento de datos de carácter personal* (conocido como *Grupo del art. 29* o *GT29*). Se trata de un órgano asesor en la materia muy importante, compuesto por expertos de los distintos estados miembros.

Por último, la Unión Europea ha culminado recientemente un largo proceso de renovación de la normativa de protección de datos con la publicación (mayo de 2016) del *Reglamento General de Protección de Datos* o *RGPD* y de algunas directivas referentes a la transmisión de datos en cuestiones judiciales y policiales, a las que no se va a referir en este trabajo.

El nuevo RGPD comenzó a ser aplicable en mayo de 2018 y, como indica su nombre, deroga la directiva 95/46/CE. Esta norma se ha convertido en una pieza clave en la evolución hacia el mundo digital y en la integración de las medidas de seguridad acordes al mismo. Se ha tomado la figura del Reglamento en vez de la Directiva porque, aunque ambas son normas vinculantes, el Reglamento tiene aplicabilidad directa en todos los Estados y permitirá alcanzar un mayor grado de homogeneización en la normativa (la Directiva exige ser traspuesta y permite a los estados un grado de discrecionalidad que, en muchos casos, genera aplicaciones sensiblemente diferentes).

El RGPD marcará las líneas fundamentales en las que se basan las metodologías propuestas en este trabajo.

2.2.2. La normativa de protección de datos en España. Evolución.

En el caso de España, el análisis normativo se debe comenzar por la *Constitución Española*, que recoge este derecho desde la perspectiva que existía en el momento de su redacción. Así, indica que “La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos” (art. 18.4 CE). Esta fórmula establece el reconocimiento a la protección de datos de carácter personal, no como un derecho autónomo, sino vinculado a otros como el honor personal y familiar. También resulta interesante resaltar que, en esa época, el uso de las tecnologías no estaba muy extendido y era percibido como un riesgo, por lo que la norma propone que su uso debía limitarse para proteger los derechos de las personas. Importante indicar también que, en el momento de promulgarse la Constitución Española, aún no se había aprobado el Convenio 108.

En el año 1992 se desarrolla este mandato constitucional con la publicación de la LORTAD (Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal). En este momento, aún perduraba, al menos en parte, esa percepción de riesgo sobre la utilización de las tecnologías.

Posteriormente, se desarrolló el derecho a la protección de datos personales con la LOPD de 1999. Esta ley, siguiendo ya la línea de la Directiva 95/46/CE, reveló un cambio de perspectiva en la medida en que eliminaba la idea de limitar el uso de las tecnologías para proteger ciertos derechos y asumió la gran importancia de la informática en el desarrollo de la sociedad. El lento desarrollo de la normativa española en la materia, hizo que la LOPD conviviera mucho tiempo con normas o desarrollos reglamentarios anteriores y fue muy compleja de implantar. De hecho, no fue hasta el año 2007, que se aprobó el reglamento que desarrolló los preceptos de esta ley. Mencionar también que esta ha sido la primera norma española acerca de esta materia que ha logrado, al menos, despertar la conciencia de la ciudadanía acerca de la protección de sus datos personales.

Pero tanto el mencionado reglamento como la LOPD han sido derogados por la nueva LOPDGDD de 2018. Esta ley ha servido para adaptar el marco normativo español al RGPD y para completar sus disposiciones. Dado que es la norma vigente actualmente, será referencia fundamental en este trabajo (junto al RGPD, que le otorga base).

Finalmente, mencionar que, para ayudar con la interpretación de la normativa vigente, la Agencia Española de Protección de Datos ha publicado diversas guías, infografías, vídeos y otras herramientas que recogen y explican los estándares y buenas prácticas relacionados con la protección de datos.

2.2.3. Otras normas relacionadas con el entorno de la investigación universitaria. Implicaciones en los tratamientos de datos personales.

- **Ley de Universidades (LOU).**

Tanto el texto de la LOU (Ley Orgánica 6/2001, de 21 de diciembre, de Universidades), como el de la posterior reforma (Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades) establecen las principales normas de funcionamiento de las universidades españolas (funciones, autonomía, naturaleza, régimen jurídico, estructura organizativa, gobierno, evaluación y acreditación, enseñanzas y títulos, investigación, estudiantes, profesorado, personal de administración y servicios, régimen económico, etc.), ya sea públicas o privadas.

En estos textos existen importantes referencias a la investigación como función de la Universidad, ya que es uno de sus objetivos esenciales.

Así mismo, en la Ley Orgánica 4/2007, en concreto en su Disposición adicional vigésimo primera, se hace referencia a la Protección de datos de carácter personal; pero es una mención muy general y basada en lo dispuesto en la derogada Ley Orgánica 15/1999.

Sin embargo, no hay ninguna regulación referente al tratamiento de datos personales en investigación.

- **Ley de la Ciencia, la Tecnología y la Innovación (LCTI).**

La LCTI (Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación) establece el marco para fomentar la investigación científica y técnica y sus instrumentos de coordinación general, con el objetivo de promocionar la investigación, el desarrollo experimental y la innovación. Así mismo, regula el *Sistema Español de Ciencia, Tecnología e Innovación* (SECTI), integrado por agentes públicos y privados que coordinan, financian y ejecutan la política de I+D+i en España.

En su Disposición adicional novena, hace referencia a la Protección de datos de carácter personal. También es una mención muy general y basada en la derogada ley 15/1999.

Importante mencionar que establece, como uno de los deberes del investigador, el "adoptar las medidas necesarias para el cumplimiento de la normativa aplicable en materia de protección de datos y confidencialidad" (art. 15 Ley 14/2011, de 1 de junio).

- **Ley de Investigación Biomédica (LIB).**

La LIB (Ley 14/2007, de 3 de julio, de Investigación Biomédica) aportó el marco normativo necesario para el desarrollo de la biomedicina, garantizando la protección de las personas afectadas por las investigaciones relacionadas.

En cuanto a la protección de datos personales, aunque también es una ley pre-RGPD y tiene en cuenta la Ley Orgánica 15/1999, aporta muchas más referencias. Señala como uno de los Principios y garantías de la investigación biomédica (art. 2.c Ley 14/2007, de 3 de julio):

> Las investigaciones a partir de muestras biológicas humanas se realizarán en el marco del respeto a los derechos y libertades fundamentales, con garantías de confidencialidad en el tratamiento de los datos de carácter personal y de las muestras biológicas, en especial en la realización de análisis genéticos

En su artículo 4 repasa los conceptos de *Consentimiento informado* y *Derecho a la información* en el ámbito de la investigación, y en su artículo 5 define las principales normas en cuanto a Protección de datos personales y garantías de confidencialidad.

Incluye los mencionados conceptos de anonimización o disociación irreversible (proceso tras el cual ya no es posible establecer la unión entre un dato y el sujeto al que se refiere utilizando recursos razonables) y el de codificación o disociación reversible (proceso en el que se sustituye o desliga la información que identifica a una persona, aplicando códigos que permitan la operación inversa).

Consentimiento. La ley establece, en su artículo 13, la obligación de obtener el consentimiento expreso, específico y escrito de una persona para realizar una investigación sobre la misma y también informar a los sujetos participantes, entre otras cosas, de las "medidas para asegurar el respeto a la vida privada y a la confidencialidad de los datos personales de acuerdo con las exigencias previstas en la legislación sobre protección de datos de carácter personal" (art. 15 Ley 14/2007, de 3 de julio).

Análisis genéticos y tratamientos de datos de carácter personal genéticos. Adelantándose a las leyes de la época, esta norma hace especial mención de los datos genéticos (considerados como especialmente sensibles por las leyes vigentes hoy día). Se incluyen distintos deberes de información, consentimiento expreso, confidencialidad, conservación, calidad, etc.

Comités de Ética de la Investigación. Esta ley referencia los Comités de Ética de la Investigación (CEI), que "deben garantizar en cada centro en que se investigue la adecuación de los aspectos metodológicos, éticos y jurídicos de las investigaciones que impliquen intervenciones en seres humanos o la utilización de muestras biológicas de origen humano" (preámbulo II Ley 14/2007, de 3 de julio). Por otro lado, en el artículo 12 se establecen una serie de condiciones en cuanto a la acreditación, funciones y condiciones de los miembros de dichos Comités de Ética de la Investigación.

- **Real decreto para la regulación de los Ensayos clínicos con medicamentos y los Comités de ética de la investigación con medicamentos.**

El RDECM (Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos) adapta la legislación nacional a las nuevas normativas europeas relacionadas con los ensayos clínicos con medicamentos para uso humano.

También es una ley pre-RGPD y contiene una estructura muy similar a la LIB desde el punto de vista de la protección de los datos personales.

Por otro lado, reconoce las funciones de los *Comités de Ética de la Investigación* (CEI) y habilita una clase especial de éstos, llamados *Comités de Ética de la Investigación con Medicamentos* (CEIm). Sobre éstos, establece las funciones relacionadas con la emisión de dictamen en estudios clínicos con medicamentos o en investigaciones clínicas con productos sanitarios, y también las condiciones de acreditación de los comités y de sus miembros.

Es importante indicar que, antes de la entrada en vigor del RD 1090/2015, los CEI y CEIm se agrupaban bajo los denominados *Comités de Ética de Investigación Clínica* (CEIC).

También fundamental, en este tipo de investigaciones, la participación de la *Agencia Española de Medicamentos y Productos Sanitarios* (AEMPS), ya que, junto con los CEIm, validará los ensayos propuestos.

- **Ley de Autonomía del Paciente (LAP).**

La LAP (Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica), entre otras funciones, se encarga de definir y regular la historia clínica de los pacientes (art. 14 Ley 41/2002, de 14 de noviembre):

> […] conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

Teniendo en cuenta que la historia clínica incorpora datos de carácter personal de diversos tipos, esta ley define cuestiones fundamentales como los posibles usos de la misma, reglas sobre la conservación de la documentación, y los derechos de acceso y custodia. Importante señalar que algunos artículos de esta ley han sido modificados por la Ley Orgánica 3/2018, de 5 de diciembre. Garantiza la preservación de los datos de identificación personal del paciente en aquellos accesos “con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia” (art. 16 Ley 41/2002, de 14 de noviembre), salvo que se cuente con el consentimiento expreso de los afectados o que se cumplan los supuestos de excepción contemplados por la LOPDGDD.

Relacionado con el derecho a la intimidad y a la protección de datos de carácter personal está el *deber de secreto* al que quedan sujetos los profesionales sanitarios para no revelar a terceros la información incluida en la historia clínica.

- **Ley del Patrimonio Histórico Español.**

La LPHE (Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español) hace una mención especial sobre la consulta pública de datos personales (incluidos los clínicos), para la que será necesario consentimiento expreso o un plazo de 25 años desde la muerte de los afectados (cuando esta fecha es conocida) o de 50 años desde la fecha de generación de los documentos que aportan los datos (art. 57 Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español).

- **Declaración de Helsinki de la Asociación Médica Mundial.**

La *Declaración de Helsinki*, promulgada por la *Asociación Médica Mundial* (AMM) es una propuesta que contiene una serie de principios éticos aplicables a la investigación médica en seres humanos. No se trata de un instrumento legal vinculante, pero es considerado como uno de los documentos más importantes a la hora de establecer guías éticas en la investigación con seres humanos. Esta declaración fue firmada originalmente en Helsinki (junio de 1964), aunque, posteriormente, ha sufrido algunas adaptaciones.

Con respecto a datos personales, la declaración indica que “deben tomarse toda clase de precauciones para resguardar la intimidad de la persona que participa en la investigación y la confidencialidad de su información personal” (Asociación Médica Mundial, 1964).

Son importantes también las recomendaciones de esta declaración con respecto a los Comités de Ética de Investigación y sobre el Consentimiento Informado (CI).

2.3. Contextualización.

Una vez analizadas, de forma somera, la evolución del marco normativo en torno a la protección de los datos de carácter personal y la aportación de las principales leyes que pueden afectar al entorno Universidad - investigación; se debe revisar el estado del arte sobre el que se deben construir las metodologías a aplicar en el campo concreto de la gestión de la protección de datos de carácter personal en proyectos de investigación universitaria.

En este trabajo, la construcción del estado del arte se plantea bajo dos perspectivas:

- Analizar las principales implicaciones legales que genera la normativa vigente en materia de protección de datos, particularizando (en su caso) sobre la construcción de metodologías de gestión de proyectos de investigación universitaria
- Analizar si ya existen metodologías establecidas y publicadas para la gestión de la protección de datos personales en proyectos de investigación universitaria.

2.3.1. Análisis de los principales efectos generados por la actual normativa de protección de datos de carácter personal.

Desde el punto de vista de la protección de datos de carácter personal es fundamental considerar el cambio que se ha producido con la entrada en vigor del RGPD. Las nuevas normativas publicadas mantienen, de forma general, la filosofía de protección definida por normas anteriores, pero añaden algunas puntualizaciones y modificaciones que es muy importante atender.

En este apartado se revisan algunas de las implicaciones del nuevo marco normativo (integrando en el análisis la normativa europea con la española), haciendo especial hincapié sobre las que pueden llegar a afectar al campo de estudio del presente trabajo.

- **Ámbito de aplicación material.**

La normativa dispuesta por el RGPD (y, por tanto, por las leyes nacionales que adaptan el ordenamiento jurídico a esta norma) “se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero” (art. 2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril).

Existen tratamientos de datos personales no afectados como, por ejemplo, las actividades que no se comprenden en el ámbito de aplicación del Derecho de la Unión, las actividades relacionadas con la seguridad nacional, política exterior y de seguridad de la Unión, actividades personales o domésticas, o las actividades con fines de prevención, investigación, detención, enjuiciamiento, etc. por parte de las autoridades competentes.

- **Ámbito de aplicación territorial.**

El gran desarrollo de los servicios prestados por Internet hace que el riesgo asociado a la protección de los datos personales asociados a dichos servicios se incremente. La globalización de la prestación de estos servicios introduce mucha complejidad a la hora de controlar los flujos de trasferencia de datos y, por este motivo, las nuevas normativas definen nuevos ámbitos de aplicación.

El RGPD determina que el ámbito territorial trasciende las fronteras de la Unión Europea, ya que la norma se aplicará a cualquier tratamiento de datos personales (art. 3 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril):

- Cuando el responsable (o encargado, en su caso) esté establecido en territorio perteneciente a la Unión, independientemente de que el tratamiento se lleve a cabo en la Unión o no.
- Cuando es aplicado sobre interesados residentes en la Unión, por parte de un responsable o un encargado no establecidos en la Unión, cuando las actividades de dicho tratamiento estén relacionadas con prácticas de oferta de bienes y servicios, o el control del comportamiento de los interesados, en la medida en que todas estas actividades tengan lugar en territorio de la Unión.
- Cuando el responsable no esté establecido en la Unión, pero lo esté en un lugar en el que se aplique el Derecho de los Estados Miembros.

Por otro lado, decir que serán sujetos obligados al cumplimento de la normativa todas aquellas organizaciones, empresas o entidades que realicen un tratamiento de datos personales a nivel comercial dentro o fuera de la Unión, siempre que ofrezcan servicios a consumidores o usuarios que estén dentro de la Unión Europea.

- **Principios.**

El RGPD mantiene, e incluso amplía, los principales ejes de protección sobre los datos establecidos históricamente.

En su artículo 5, se desarrollan los *Principios relativos al tratamiento*. Es un texto fundamental, ya que condiciona la base sobre la que debe aplicarse cualquier tratamiento y que será muy tenido en cuenta en este trabajo. Se incluyen los siguientes principios fundamentales:

- *Licitud*. En el artículo 6, se definen las condiciones de la *Licitud del tratamiento*. Lo más importante para que un tratamiento sea lícito es contar con el consentimiento explícito y expreso del interesado (figura que se refuerza en este texto) o bien con alguna otra base legitimadora establecida conforme a Derecho. Los considerandos 44 a 50 incluyen situaciones de consentimientos lícitos y el artículo 7, algunas condiciones del otorgamiento y su retirada. En el artículo 8, se definen las condiciones aplicables al consentimiento de los niños en relación a los servicios de la sociedad de la información.
- *Lealtad y transparencia en relación con el interesado*. El tratamiento leal implica transparencia en la aplicación de los tratamientos y también en la exposición de motivos de licitud para la recogida y uso de los datos. Los tratamientos deben ser

explicados a los interesados de una forma accesible, concisa y con un lenguaje fácilmente entendible. Esta condición se ha endurecido con la nueva normativa.

- *Limitación de la finalidad*. El RGPD exige que se han de asegurar "fines determinados, explícitos y legítimos", garantizando que no existan tratamientos posteriores con otros fines. Importante mencionar que también se recoge la excepción de poder aplicar tratamientos posteriores si éstos tienen, entre otros, "fines de investigación científica e histórica o fines estadísticos" (art. 5.1.b Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril).
- *Minimización de los datos*. Los datos personales deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" (art. 5.1.c Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril). No se deben solicitar más datos que los que estrictamente se necesitan.
- *Exactitud*. Los datos deben ser exactos y, en caso de haberse producido cambios sobre los mismos, deben actualizarse. El responsable deberá aplicar los medios necesarios para, de un modo razonable, permitir esta corrección y/o actualización.
- *Limitación del plazo de conservación*. Los datos deben ser conservados durante el tiempo necesario para cumplir los fines declarados para el tratamiento. Más allá de ese tiempo, se podrán conservar si se anula la posibilidad de identificación de los interesados o si pasan a tratarse exclusivamente con "fines de archivo en interés público, fines de investigación científica o fines estadísticos", bajo ciertas condiciones (art. 5.1.e Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril).
- *Integridad y confidencialidad*. Es necesario aplicar medidas de seguridad adecuadas (técnicas u organizativas) que protejan los datos contra tratamientos no autorizados y contra su pérdida, destrucción o daño accidentales.
- *Responsabilidad proactiva (accountability)*. Se trata de un principio muy importante, y también novedoso, por el cual el responsable deberá garantizar y ser capaz de demostrar que todos los anteriores principios se cumplen. Para ello, deberá aplicar todas las medidas técnicas y organizativas necesarias que garanticen la efectiva protección de los datos personales en cuestión. El objetivo es fomentar una actitud preventiva en vez de reactiva en la protección de los datos por parte de los responsables y encargados, en su caso.

- **Categorías especiales de datos.**

En cuanto al tratamiento de categorías especiales de datos personales, el RGPD define:

- Por un lado, los tipos de datos que integran esta tipología, a saber (art. 9 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril):

  > datos personales que revelen 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 las orientaciones sexuales de una persona física

  Es importante destacar la ampliación del catálogo de datos sensibles o categorías de datos personales especiales, sumando nuevos tipos como los datos genéticos o los biométricos.
- Y, por otro, las distintas circunstancias en las que se permite el tratamiento de este tipo de datos. No se analizarán en profundidad las casuísticas de este artículo, pero es importante mencionar que:
  - El apartado 9.2.a) indica que los datos de categoría especial se pueden tratar si el interesado otorga su consentimiento explícito para ello (excepto que alguna otra norma del Derecho de la Unión o de los Estados miembros lo prohíba expresamente).
  - En el apartado 9.2.j) se indica que es posible realizar tratamientos de datos personales de categoría especial con “fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos”, teniendo en cuenta las garantías previstas en el artículo 89.1), y siempre que se respete el derecho a la protección de datos y se establezcan las medidas adecuadas para proteger los intereses y derechos de los interesados.

- **Datos relativos a condenas e infracciones penales.**

Según el RGPD, este tipo de tratamientos sólo se podrá llevar a cabo “bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros” (art. 10 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril).

- **Personas fallecidas.**

El RGPD deja muy claro que, en el caso de los datos personales sobre personas fallecidas, no se deben aplicar las regulaciones establecidas en el mismo: “debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe ser de aplicación a personas fallecidas.” (considerando 158 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril). Además, deja abierta la puerta a una regulación más concreta en materia de creación científica relacionada con los fallecidos. Esto

quiere decir que cuando la investigación histórica alcanza a personas fallecidas, quedaría fuera del alcance de esta norma.

- **Tratamientos que no requieren identificación.**

Previstos en el artículo 11 del RGPD, se refieren a aquellos datos en los casos en los que "no requieren o ya no requieren la identificación del interesado". En esos casos, ya no serán de aplicación los artículos 15 a 20 del RGPD (derechos del interesado).

- **Legitimación: consentimiento.**

Uno de los pilares en la normativa de protección de datos personales es el consentimiento, ya que es la principal vía de legitimación de los tratamientos.

El RGPD especifica que (considerando 32 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril)

> El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen […] El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines.

El artículo 4 del RGPD define consentimiento y el 7 establece las condiciones para la prestación de un consentimiento legítimo por parte de los titulares de los datos:

- El responsable debe poder demostrar que el titular prestó su consentimiento.
- El consentimiento solicitado para más de un asunto en el contexto de una declaración escrita debe informarse debidamente. Si los datos se utilizarán para varias finalidades, debe constar claramente que el consentimiento se aplica para todas ellas.
- El consentimiento debe poder ser revocable en cualquier momento.
- Para determinar si un consentimiento se ha prestado libremente, entre otras cosas, se tendrá en cuenta si la ejecución de un contrato se supedita al consentimiento del tratamiento de datos personales que no son necesarios para la correcta ejecución de dicho contrato.

El consentimiento debe ser informado, es decir, deben primar los principios de transparencia y lealtad a la hora de informar al interesado, paso previo a la prestación del consentimiento. El artículo 13 del RGPD precisa la información concreta a facilitar por parte del responsable. Desde las distintas Autoridades de Protección de Datos se recomienda adaptar un modelo de información por capas o niveles para hacer compatibles, por un lado, la concisión y facilidad

de comprensión de la información y, por otro, el mayor volumen y precisión exigidos a la misma.

Existe una regulación específica para el consentimiento en el caso de los niños.

- **Derechos de los interesados.**

El RGPD refuerza, de forma clara, los derechos de los interesados, incluyendo algunos nuevos y otorgando más importancia a los ya existentes. Esto se traduce en una mejora sustancial de la capacidad de decisión, control y gestión de los interesados sobre los datos que confían a terceros. El responsable del tratamiento estará obligado a atender cualquier solicitud de ejercicio de derechos y es muy importante que cuente con las herramientas adecuadas para poder hacerlo.

La nueva lista de derechos del interesado es la siguiente:

- *Información*. Artículos 13 y 14 RGPD y 11 LOPDGDD.
- *Acceso*. Artículos 15 RGPD y 13 LOPDGDD.
- *Rectificación*. Artículos 16 RGPD y 14 LOPDGDD.
- *Supresión o derecho al olvido*. Artículos 17 RGPD y 15 LOPDGDD.
- *Portabilidad*. Artículos 20 RGPD y 17 LOPDGDD.
- *Oposición*. Artículos 21 RGPD y 18 LOPDGDD.
- *Limitación del tratamiento*. Artículos 18 RGPD y 16 LOPDGDD.
- *Oposición a ser objeto de decisiones individuales automatizadas*. Artículos 22 RGPD y 18 LOPDGDD.

- **Medidas de cumplimiento.**

Desde el punto de vista de los sujetos obligados, el RGPD plantea una serie de obligaciones y medidas de seguridad (artículos 24 a 36):

- Correcta definición de las figuras del responsable, corresponsable y encargado del tratamiento.
- Registro adecuado de todas las actividades de tratamiento llevadas a cabo, incluyendo toda la información obligatoriamente requerida para dicho registro. Este registro es ahora interno y ya no es necesario que se comunique a la autoridad de control.
- *Protección de datos desde el diseño y por defecto*. Todos los procedimientos y herramientas diseñados para realizar una actividad de tratamiento de dados de carácter personal deberán incorporar desde el primer momento y por defecto todas

aquellas medidas necesarias para garantizar la protección de los derechos de los interesados.

- Medidas de seguridad que garanticen *Integridad*, *Confidencialidad*, *Disponibilidad* y *Resiliencia* de los datos asociados al tratamiento. El responsable y/o encargado deberá aplicar todas aquellas medidas de seguridad y organizativas necesarias para garantizar estas tres características fundamentales de la información. Dentro de este conjunto de medidas, cabe destacar todas aquellas que incluyen procesos de *cifrado*, *seudonimización* y *backup*.
- Comunicación de brechas o incidentes de seguridad a la correspondiente autoridad de control y a los interesados afectados.
- Realización de procedimientos EIPD (*Evaluación de Impacto relativa a la Protección de Datos*) o, en inglés, PIA (*Privacy Impact Assessment*) en aquellos casos en que exista un riesgo elevado en la protección de los derechos de los interesados con respecto a sus datos personales. Se trata de una nueva y fundamental obligación que incorpora procedimientos recogidos de las modernas metodologías de análisis y gestión de riesgos. Su objetivo es permitir que el propio responsable del tratamiento pueda determinar los riesgos asociados a cada tratamiento y así definir las medidas adecuadas para garantizar la protección de los datos afectados.
- Cooperación y consultas a las autoridades de control pertinentes en los casos en los que se detecten riesgos importantes en determinados tratamientos de datos.

- **Delegado de Protección de Datos (DPD).**

Otra de las novedades del RGPD es la incorporación de la figura del *Delegado de Protección de Datos* (DPD o DPO, por sus siglas en inglés, *Data Protection Officer*), recogida en los artículos 37 a 39, y en el considerando 97 (obligatoriedad de nombramiento, designación, posición, funciones, posibilidades de intervención, nivel de conocimientos, etc.). La LOPDGDD detalla con un poco más de profundidad algunas de estas cuestiones en sus artículos 34 a 37.

Según el *Esquema de Certificación de Delegados de Protección de Datos de la AEPD* (Agencia Española de Protección de Datos, 2018), el perfil del puesto de DPD tendrá, como mínimo, las siguientes funciones:

- Informar y asesorar al responsable o, en su caso, al encargado del tratamiento sobre las obligaciones que les incumben, ya sea en virtud del RGPD o por otras disposiciones.

- Supervisar el cumplimiento de todo lo dispuesto en el RGPD y en otras disposiciones, así como de las políticas del responsable o encargado del tratamiento en materia de protección de datos personales.
- Supervisar la asignación de responsabilidades en la materia.
- Supervisar la concienciación y la formación del personal que colabora en las operaciones de tratamiento.
- Supervisar las auditorías en la materia.
- Ofrecer el asesoramiento adecuado en las EIPD y supervisar su aplicación.
- Cooperar con las autoridades de control.
- Actuar como punto de contacto con las autoridades de control y en especial en las consultas previas cuando una actividad de tratamiento suponga un riesgo alto.
- Realizar otras consultas a las autoridades de control.

- **Contratos entre responsables y encargados del tratamiento.**

Aunque las figuras de responsables y encargados del tratamiento no han variado con la entrada en vigor de las nuevas normativas, sí que se han reforzado las características que deben presentar los contratos de acceso a datos por parte de los encargados (art. 28 RGPD). Es muy importante reflejar adecuadamente las funciones a desempeñar por parte del encargado y las medidas que deberá tomar para garantizar los derechos de los interesados.

La AEPD ha publicado la guía *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento* (Agencia Española de Protección de Datos, 2017a), con el objetivo de facilitar la redacción de dichos contratos.

- **Régimen sancionador.**

El RGPD ha procurado establecer un criterio más uniforme en la imposición de sanciones, tanto en relación con los preceptos infringidos como en las cuantías de dichas sanciones.

El artículo 83 regula tanto los objetivos de las sanciones como las circunstancias agravantes o atenuantes en su aplicación. Cada Estado Miembro podrá establecer normas internas sobre otras sanciones aplicables, especialmente las que no estén recogidas en el propio RGPD.

Es fundamental señalar que se ha producido un significativo aumento en la cantidad económica de las sanciones con respecto a la regulación anterior. La explicación está en que se deben adaptar tanto al tamaño de las entidades (las multas hasta ahora podrían ser insignificantes para determinados tipos de entidades internacionales) como al elevado riesgo que comporta el manejo inseguro de las grandes cantidades de datos personales que la actual organización social exige.

- **Tratamiento de datos relativos a la investigación en salud.**

El RGPD define como datos personales relativos a la salud aquellos "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" (art. 4 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril). En este sentido, el Grupo de Trabajo del Artículo 29[1] ha matizado la definición, aclarando que también incluye aquellos datos íntimamente ligados con el estado de salud de la persona, incluyendo los datos genéticos o aquellos sobre el consumo de medicinas o fármacos.

Por otro lado, el RGPD define, de forma amplia, el tratamiento de datos con fines de investigación científica. Incluye, entre otros, "el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado" (considerando 159 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril).

Se otorga una regulación especial a este tipo de tratamientos con el objetivo de que la normativa de protección de datos general no suponga una barrera insalvable para llevar a cabo este tipo de investigaciones, dados los grandes beneficios que suponen para la sociedad. Por eso, el artículo 89 incluso prevé la posibilidad de limitar los derechos de acceso, rectificación, limitación y oposición en aquellos tratamientos con fines de investigación que cumplan las garantías adecuadas (disponer de medidas técnicas y organizativas, principio de minimización, aplicación de seudonimización).

Como complemento, la LOPDGDD establece los criterios fundamentales que deben guiar los tratamientos de datos personales en el área de la investigación en salud. Según este texto, cabe destacar los siguientes (disposición adicional decimoséptima LO 3/2018, de 5 de diciembre):

- Licitud:

  a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica.
  b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.
  c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad

[1] El *Grupo de Trabajo del Artículo 29* fue creado en virtud del artículo 29 de la Directiva 95/46/CE, con fines consultivos en materia de protección de datos. Tras la publicación del RGPD, el *Comité Europeo de Protección de Datos* continúa la labor de dicho grupo.

concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. […]
d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

- Excepciones a la ejecución de derechos del interesado:

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (UE) 2016/679 cuando:
1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.
2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.
3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

- Otras obligaciones en tratamientos con fines de investigación en salud pública y biomédica:

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:
1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.
2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.
3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.
4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

- Otros:

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial. En defecto de la existencia del mencionado Comité, la entidad

responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

2.3.2. Análisis de las principales metodologías existentes para la gestión de la protección de datos personales en proyectos de investigación universitaria.

Se ha realizado una búsqueda de documentación, en los repositorios de información de las distintas universidades españolas, sobre metodologías concretas enfocadas a la gestión de la protección de los datos personales en proyectos de investigación. Los resultados obtenidos de dicha búsqueda han sido negativos, por lo que se llega a la conclusión de que las universidades o no disponen de metodologías concretas en esta materia o bien, si las tienen, son internas o privadas.

Se han podido identificar, sin embargo, diversas publicaciones (sólo en algunas universidades) sobre procedimientos (instrucciones básicas, formularios, etc.) que podrían tener cierta relación, ya que se refieren a instrucciones sobre la gestión de algunos tipos de proyectos de investigación con respecto a la evaluación por parte de los comités de ética y a la obtención del consentimiento informado. Este tipo de normativas, dado el área temática en que se circunscriben, incluyen algunas referencias a la protección de datos personales (algunas incluso continúan aludiendo a la antigua normativa), pero son muy básicas y resultan insuficientes para cubrir los requisitos propuestos por el RGPD.

Algunos ejemplos de este tipo de publicaciones se pueden encontrar en los siguientes enlaces (recopilados en diciembre de 2019):

- Universidad Pablo de Olavide (Sevilla). https://www.upo.es/area-investigacion/comite-etico/procedimiento-humanos/?imprimible
- Universidad Politécnica de Valencia. https://www.upv.es/entidades/VIIT/info/892853normalc.html
- Universidad de Alicante. https://sstti.ua.es/es/comite-etica/presentacion.html
- Universidad de León. https://www.unileon.es/investigadores/comite-etica
- Universidad de Granada. https://investigacion.ugr.es/pages/etica
- Universidad Autónoma de Madrid. https://www.uam.es/UAM/ComEt-Presentacion/1446745195080.htm?language=es&nodepath=Presentaci?n

Por otro lado, es conveniente mencionar otras publicaciones que pueden aportar cierta ayuda en esta materia:

- **Horizon 2020 Programme Guidance. How to complete your ethics self-assessment. European Commission.**

Horizon 2020 (Programa Marco Horizonte 2020) es un importante programa de financiación de la UE para distintos proyectos de investigación en el período 2014-2020, regulado en el Reglamento (UE) nº 1291/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, así como en el Reglamento (UE) nº 1290/2013 del Parlamento Europeo y del Consejo de 11 de diciembre de 2013 por el que se establecen las normas de participación y difusión aplicables a Horizonte 2020.

Para solicitar la participación en este programa, es necesario cumplimentar (por parte del investigador encargado de la gestión) una serie de documentos entre los que se incluye el *Proposal Submission Forms*. En el apartado 4 de esta memoria se incluye la *Ethics issues table*, que contiene una serie de 'checklists' sobre si la investigación incluirá -entre otros ítems- participación de humanos, si se tratarán células humanas, o si se tratarán datos personales. En función de si la respuesta es positiva o negativa, las guías indican la información y/o documentación a aportar; y añaden información detallada para solventar los posibles problemas (European Commission, 2019).

Estos datos son evaluados por expertos independientes, que examinan las solicitudes para comprobar si cumplen los principios éticos y las normativas de protección de datos, investigación biomédica, etc.

- **Guía de buenas prácticas en materia de Transparencia y Protección de Datos. CRUE Universidades Españolas.**

Encargada por *CRUE - Secretarías Generales* al *Grupo de Trabajo de Gabinetes Jurídicos*, la *Guía de buenas prácticas en materia de Transparencia y protección de Datos* tiene como objetivo facilitar la tarea de determinar cuándo prevalece el derecho de acceso (previsto por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno) y el de protección de datos de carácter personal (previsto por el RGPD y la LOPDGG). Se trata de una herramienta orientativa, no vinculante, y abierta (sujeta a futuras aportaciones, revisiones y modificaciones).

En el epígrafe "Actividad investigadora y de transferencia del conocimiento" aporta varias recomendaciones sobre los siguientes temas (CRUE Universidades Españolas, 2019):

- “Publicidad activa”. Información orientativa que debería ser publicada por las instituciones según el marco normativo de transparencia que les sea de aplicación.
- “Realización de estudios”. Catálogo de posibilidades de acceso a datos de archivos históricos, datos de contacto de personal docente o estudiantes, cesiones de datos de estudiantes y profesorado, cesión de datos entre administraciones y, muy importante, sobre tratamientos de datos en la investigación en salud. Con referencia a este último tratamiento, remite a las normas previstas por el RGPD (con especial hincapié en los procesos de seudonimización) y hace referencia a los informes que se deben generar por parte de los Comités de Ética de la Investigación de las entidades que intervienen (CRUE Universidades Españolas, 2019).
- “Acceso a material científico”. Recomendaciones para el acceso a la producción científica de los investigadores. Es necesario un equilibrio entre las publicaciones con acceso abierto impulsadas por la LCTI, la conexión con la transparencia pública, la protección de los derechos de propiedad intelectual, etc. (CRUE Universidades Españolas, 2019).
- “Difusión de noticias”. Tratamiento lícito de difusión a través del correo electrónico de convocatorias e informaciones sobre la actividad investigadora (CRUE Universidades Españolas, 2019)
- “Acceso a información relativa a proyectos de investigación”. Difusión lícita relativa a los catálogos de proyectos llevados a cabo por cada universidad.

2.4. Problemáticas.

Un pequeño resumen de las problemáticas que se han planteado durante la confección de este trabajo es el siguiente:

- A nivel general, aunque la sociedad va tomando conciencia poco a poco, aún no existe una adecuada cultura de protección de datos personales. Esto supone que, aunque muchas personas ya son conscientes de que disponen del derecho de protección de sus datos personales, aún no tienen una visión completa de lo que implica ese derecho ni tampoco cómo ejercitarlo. Esto afecta tanto a investigadores como a las personas cuyos datos personales se tratan en los proyectos de investigación (interesados).
- Las normativas en relación con la protección de datos publicadas hasta la fecha han sido muy generales en muchos aspectos, es decir, no han ofrecido un grado de concreción adecuado con respecto a muchos de los procedimientos que proponen. Han sido las distintas autoridades de control territoriales las que han tenido que ampliar la interpretación de las mismas. Ocurría con la anterior normativa y también con la nueva.

- Las últimas regulaciones sobre protección de datos personales han sido publicadas hace relativamente poco tiempo y, para algunas de sus posibles implicaciones, no existen aún adaptaciones, explicaciones, o desarrollos suficientes (por ejemplo, por parte de la AEPD).
- Ya en el entorno universitario, los grupos de trabajo activados por las universidades españolas (CRUE) para desarrollar criterios comunes en esta materia son muy jóvenes. El trabajo en esta línea ha comenzado hace muy poco tiempo y los resultados aún son escasos.
- El grado de concreción de las normativas que regulan los procesos de investigación universitaria en las materias relacionadas con el objeto de estudio de este trabajo es muy bajo. Hay muchas cuestiones que quedan relegadas a la interpretación de las normativas en la materia vigentes en cada momento.
- El acceso al entorno de investigación universitario por parte del autor de este trabajo ha estado ligeramente limitado. Por cercanía, se han realizado diversas consultas con una universidad privada pequeña española, cuyas cifras relativas a procesos de investigación son muy discretas. Aunque se ha podido obtener información sobre procesos, modos de trabajo, etc., el modesto volumen investigador de dicho centro ha condicionado los resultados de la validación de la metodología.
- En este documento se ha utilizado, por defecto, el sistema APA II para citar y referenciar. Sin embargo, dado que no existen pautas claras de normalización en el caso de la legislación, se ha optado por citar los textos legales incluyendo, entre paréntesis: la ubicación de la cita dentro del texto de la norma (artículo, considerando, etc.), el nombre abreviado de la norma y la fecha de su publicación. Esto puede acarrear algunos problemas de identificación de las citas por parte de los sistemas anti-plagio.

3. Objetivos concretos y metodología de trabajo.

3.1. Objetivo general.

El objetivo general de este trabajo es, como ya se ha mencionado, elaborar una metodología aplicable a la realización de las tareas administrativas y de gestión relacionadas con los tratamientos de datos de carácter personal incluidos en los proyectos de investigación universitaria que permita a los investigadores realizar estos trámites de forma fácil y segura, para así dedicar sus esfuerzos a las tareas directamente relacionadas con el fondo de sus proyectos, que son para las que están especialmente preparados.

3.2. Objetivos específicos.

En cuanto a los objetivos específicos, se pueden señalar los siguientes:

- Obtener una visión lo más amplia posible sobre la regulación en materia de protección de datos.
- Obtener información sobre los procesos de gestión de los proyectos de investigación universitaria y analizar las implicaciones de la regulación en materia de protección de datos en la gestión de dichos proyectos.
- Diseñar y desarrollar los elementos que deben componer la metodología objeto del trabajo.
- Evaluar la metodología.
- Obtener conclusiones y exponer líneas futuras de trabajo.

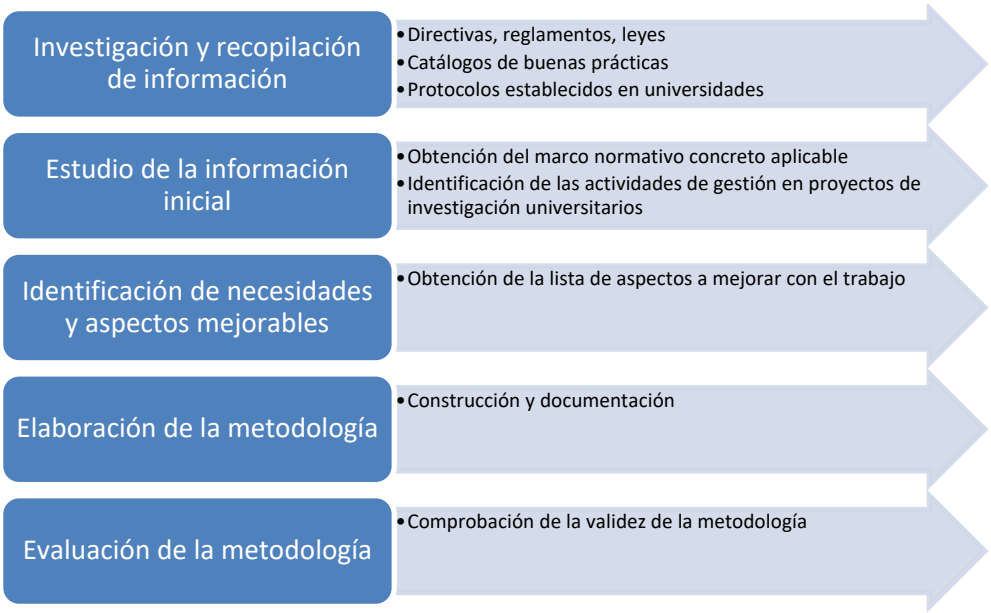
3.3. Metodología del trabajo.

Teniendo en cuenta que este trabajo es de tipo “desarrollo de metodología”, los pasos a realizar para desarrollar la contribución que permita alcanzar los anteriores objetivos, el trabajo se estructura en cinco fases:

1. Fase de investigación y recopilación de información. En esta fase se recopilan todas las normativas, catálogos de buenas prácticas, protocolos establecidos por las distintas entidades, etc., que puedan afectar a la regulación del objeto de estudio.
2. Fase de estudio y procesado de la información obtenida. Con la información obtenida en la etapa anterior, se plantea, por un lado, el marco normativo sobre el que se construirá la metodología y, por otro, la identificación de todas las actividades de gestión relacionadas con los proyectos de investigación universitarios.

3. Fase de identificación de necesidades no cubiertas o aspectos mejorables. Planteado el marco normativo y las actividades de gestión de los proyectos de investigación, se buscan todos aquellos aspectos no regulados específicamente y las actividades a estandarizar y/o asegurar.
4. Fase de elaboración de la metodología. Basada en los resultados de la fase anterior, se construye y documenta la metodología.
5. Fase de evaluación de la metodología. Comprobación de que la metodología es válida, es decir, si cumple el objetivo de asegurar y facilitar las tareas de gestión a los investigadores universitarios, desde el punto de vista del tratamiento de los datos personales.

Figura 1. Descripción de la metodología de trabajo para desarrollar este proyecto.



Fuente: elaboración propia

4. Desarrollo de la contribución.

4.1. Identificación de requisitos.

Como se ha comentado anteriormente, el problema principal a tratar con la metodología que seguidamente se expone, es la incorrecta adaptación a las nuevas normativas (RGPD, LOPDGDD y derivados) de los procesos de gestión en proyectos de investigación universitaria que incluyen tratamientos de datos personales. Esta gestión es llevada a cabo, generalmente, por los propios grupos de investigación y, dependiendo de la preparación o recursos de los gestores, el resultado podría llegar a ser lesivo para los derechos en materia de protección de datos personales de los interesados implicados en la investigación.

El contexto para el que se va a tratar de ajustar la metodología es el de grupos de investigación asentados en universidades pequeñas-medianas españolas, ya que en estos ámbitos es probable que los recursos puestos a disposición de los investigadores sean más reducidos y la ayuda será mejor recibida.

Para implementar correctamente la metodología desarrollada en esta memoria se identifican, fundamentalmente, tres tipos de requisitos: legales, organizativos y de formación.

4.1.1. Requisitos legales.

En el apartado 2 de esta memoria se incluye un amplio estudio de las normas legales y recomendaciones aplicables a la materia estudio, así como la justificación de las mismas.

De forma resumida, se puede indicar que la metodología para la gestión de datos personales en proyectos de investigación universitaria deberá atenerse a lo dispuesto en las siguientes normas fundamentales:

- RGPD.
- LOPDGDD.

Y, aunque no son normas específicas en materia de datos personales, también deberá atenerse, en algunos aspectos, a las siguientes:

- LOU.
- LCTI.
- LIB.
- RDECM.

Por tanto, todos los contenidos reunidos en esta contribución se ajustarán a lo dispuesto en los mencionados textos legales.

4.1.2. Requisitos organizativos.

Para elaborar la contribución expuesta en esta memoria, es necesario adaptarse a los esquemas de gestión de los proyectos de investigación habituales en el entorno universitario. Esta gestión será distinta en función de su clasificación ética, metodológica y legal, y también de si el proyecto incluye o no tratamientos de datos de carácter personal.

Evidentemente, existen muchos tipos de proyectos de investigación. La Agencia Estatal de Investigación (AEI) identifica hasta 19 áreas para organizar los procesos de investigación en España. Existen áreas como *Psicología* (PSI), *Biociencias y biotecnología* (BIO) o *Biomedicina* (BME) en las que es fundamental trabajar con humanos y pueden incluirse tratamientos de datos personales, y otras áreas como *Derecho* (DER), *Ciencias y tecnologías de materiales* (MAT) o *Energía y transporte* (EYT), en las que es menos probable trabajar con datos personales (Agencia Estatal de Investigación, s. f.).

Aunque el proceso es relativamente complejo, dependiendo del tipo de proyecto y de las normativas que le puedan afectar en función de la materia de estudio, la gestión administrativa inicial general de un proyecto de investigación estándar (sin profundizar en protección de datos personales) se podría esquematizar en un modelo como el siguiente:

1. El investigador universitario desea realizar un proyecto. En primer lugar, debería consultar con el órgano de gestión de la investigación en su universidad. Dicho órgano debería establecer si el proyecto es pertinente a nivel interno o no (teniendo en cuenta los objetivos propios de cada universidad). Este órgano, así mismo, debería establecer un primer filtro de cara a garantizar el cumplimiento de las normas aplicables en función del tipo de proyecto.
2. Una vez obtenida la autorización inicial interna del proyecto, se debería identificar la tipología del mismo para poder solicitar la correspondiente evaluación ética, metodológica y legal, teniendo en cuenta la siguiente clasificación:
    a. El proyecto no incluye investigación con humanos. Opciones:
        i. El proyecto investiga con animales. Para su evaluación, se deberá remitir al *Comité de Ética de Experimentación Animal* (CEEA) correspondiente.
        ii. El proyecto no investiga con humanos (ni con los datos personales asociados a éstos) ni con animales, pero incluye (o puede incluir) tratamientos de datos personales de forma accesoria y/o accidental.

Para su evaluación, se deberá remitir al *Comité de Ética de la Investigación* (CEI) correspondiente.

iii. El proyecto no investiga con humanos ni con animales y tampoco incluye tratamientos de datos personales de ningún tipo. Su validación no requiere procedimientos especiales (al menos, desde el punto de vista ético, metodológico y legal, y/o de gestión de datos personales) y dependerá, exclusivamente, del órgano de gestión de la investigación de la universidad afectada.

b. El proyecto incluye investigación con humanos. Opciones:

i. El proyecto se basa en experimentos no clínicos en los que intervienen humanos, es decir, no está afectado por las estrictas normativas de la investigación en materia de salud, pero requiere alguna interacción básica con humanos y el tratamiento de sus datos personales. Para su evaluación, se deberá remitir al *Comité de Ética de la Investigación* (CEI) correspondiente. Requerirá consentimiento informado de los afectados.

ii. El proyecto se basa en procedimientos invasivos[2] en humanos o en la utilización de cualquier tipo de muestras biológicas (incluyendo células troncales, preembriones o cualquier otro tipo de muestras biológicas humanas que puedan dar lugar a la obtención de material celular embrionario) . Para su evaluación, se deberá remitir al *Comité de Ética de la Investigación* (CEI) correspondiente. Requerirá consentimiento informado de los afectados.

iii. El proyecto se basa en investigación clínica con medicamentos o productos sanitarios. Para su evaluación, se deberá remitir al *Comité de Ética de la Investigación con medicamentos* (CEIm) correspondiente. En el caso de los medicamentos, también requiere aprobación de la *Agencia Española de Medicamentos y Productos Sanitarios* (AEMPS). Requerirá consentimiento informado de los afectados.

3. Clasificado el proyecto, se remite solicitud de evaluación al organismo correspondiente. Obtenida esta validación, se podrá comenzar con los trabajos asociados al mismo.

[2] Procedimiento invasivo: todo aquel procedimiento a través del cual el cuerpo humano sufre la penetración física o ‘invasión’ de dispositivos médicos como agujas, sondas, endoscopios u otros aparatos.

4.1.3. Requisitos de formación.

La materia tratada en este estudio es compleja y, para poder abordarlo con garantías, ha sido necesario para el autor adquirir conocimientos muy específicos en materia de protección de datos de carácter personal.

Por otro lado, y dado que puede ocurrir que los investigadores no posean los suficientes conocimientos sobre este campo, se entiende como fundamental que, para la aplicación de la metodología propuesta, los investigadores reciban una formación previa sobre protección de datos personales. Al menos, es necesario comprender los conceptos revisados en los apartados 2.1 y 2.3.1 de esta memoria, ya que la metodología hará amplio uso de ellos.

Evidentemente, los investigadores también deberán poseer conocimientos legales específicos sobre los campos de gestión en su área de investigación.

4.2. Descripción de la metodología.

Una vez planteados los requisitos de la metodología, se pasa a la descripción de la misma.

La aplicación de la metodología arranca simultáneamente con el diseño del esquema de gestión administrativa del proyecto. Durante la tarea de organización inicial del proyecto se deben identificar –si los hay- todos los tratamientos de datos personales que éste debe incorporar y de esta identificación derivan todos los demás trabajos. La metodología se organiza describiendo una serie de fases que, para su correcta implementación, deberán ser ejecutadas por los gestores de cada proyecto de investigación.

4.2.1. Fases de la metodología.

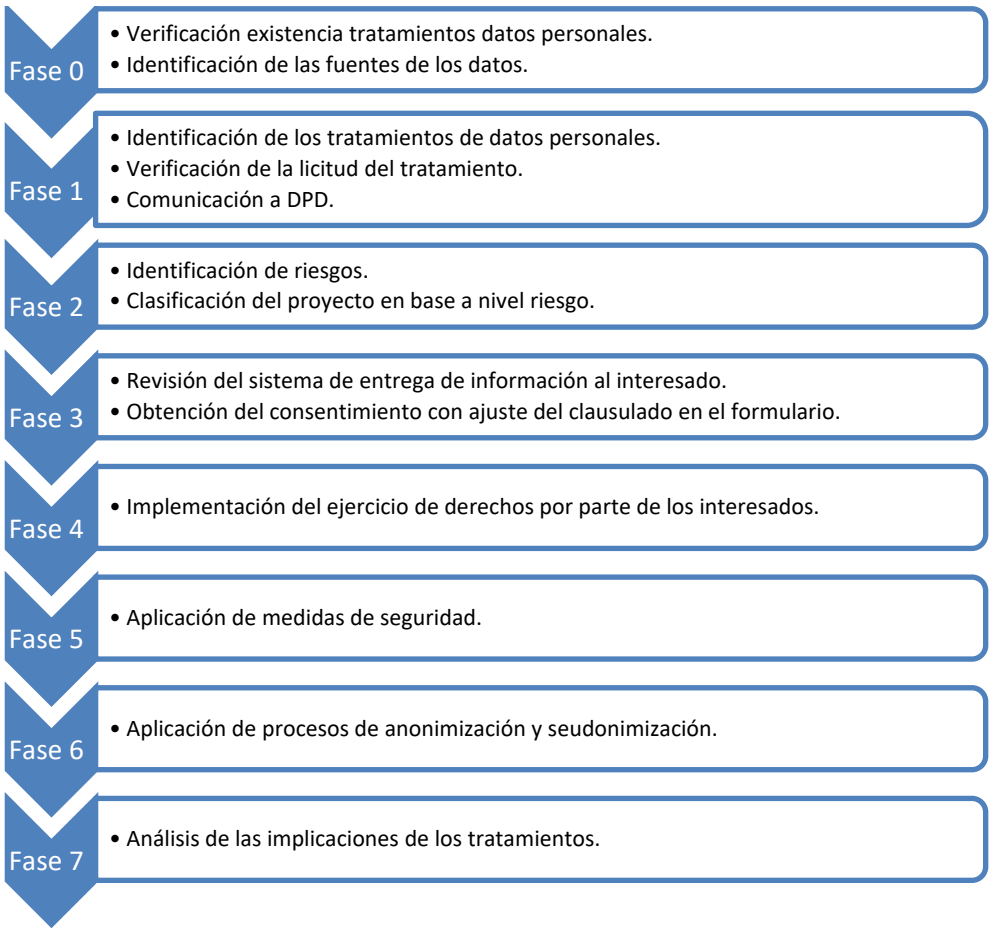
El investigador principal (o aquél encargado de gestionar administrativamente el proyecto), deberá seguir los pasos descritos en las siguientes fases para asegurar que dicho proyecto se adecúe a la normativa en materia de protección de datos de carácter personal.

Se trata de una metodología a aplicar en los momentos iniciales del proyecto. De hecho, ejecutar ciertas fases de la misma ayudarán a obtener parte de los datos necesarios para la evaluación ética, metodológica y legal del proyecto (de acuerdo con el esquema propuesto en el punto 4.1.2 de esta memoria). Es conveniente que las distintas fases se apliquen en el orden previsto.

Seguidamente, se expone una representación teórica de la metodología, adecuada a la exposición en un trabajo académico. En una fase posterior (que se explicará en el apartado de líneas futuras de trabajo), se deberían recoger los contenidos de la misma y plasmarlos en un documento preparado para su utilización directa por parte de los investigadores. En este

documento, se aplicaría un lenguaje menos técnico, se elevarían los niveles de detalle en determinadas instrucciones, se incluirían gráficos de apoyo, etc.

Figura 2. Fases de la metodología propuesta.



Fuente: elaboración propia.

- **Fase 0. Verificación de la existencia de tratamientos de datos personales e identificación de las fuentes de los mismos.**

Uno de los pasos fundamentales en el inicio de la gestión de un proyecto de investigación es verificar si en el mismo se van a realizar tratamientos de datos personales o no. Tomando como base las definiciones reflejadas en el apartado 2.1 de esta memoria, el investigador

deberá considerar que existe tratamiento de datos si se cumplen, simultáneamente, las tres condiciones siguientes:

1. El proyecto incluye el trabajo con cualquiera de los tipos de información descritos en la definición de dato de carácter personal, pertenecientes a personas sobre las que se realiza el estudio objeto del proyecto[3].
2. La información contenida en los datos mencionados identifica directamente a las personas a quien pertenecen o bien, aunque no las identifique directamente, puede servir para identificarlas, mediante la utilización de un conjunto razonable de recursos técnicos (o de otro tipo).
3. Los datos gestionados pertenecen a personas no fallecidas.

Existen multitud de líneas de investigación en las que únicamente se utilizan datos *anonimizados* o *disociados* y en esos casos no hay tratamiento de datos personales como tal, porque, aunque se utilicen datos que pertenecen a personas (se cumple la primera condición), es imposible asociarlos con individuos concretos y, por lo tanto, el derecho a la intimidad y a la protección de sus datos se mantiene. El tratamiento de este tipo de información ya no está afectado por el RGPD y sus normas de desarrollo (considerando 26 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril). Normalmente, esta anonimización se consigue eliminando todos los datos identificativos del conjunto de datos personales con el que se trabaja. En muchos casos, estos procesos de anonimización y seudonimización se aplican como fase previa a la publicación de los resultados de la investigación.

Por otro lado, es necesario identificar las fuentes de los datos personales. Las principales opciones en este ámbito son:

- Obtención de nuevos datos para el proyecto directamente de los interesados.
- Obtención de los datos desde otros tratamientos previos (relacionados con el proyecto de investigación o no). En estos casos se produce una cesión que debe estar legitimada desde el tratamiento origen o bien incluida en alguno de los supuestos de cesión para investigación recogidos en la LOPDGDD (disposición adicional decimoséptima). Tipos:
    - Datos completos. Se ceden todos los datos desde el tratamiento original (existe identificación de los interesados).

[3] La manipulación de los datos personales pertenecientes a los miembros del equipo de investigación, colaboradores y otro personal interviniente en el proyecto también es considerado un tratamiento de datos, pero se considera como accesorio o externo al proyecto, es de bajo riesgo y su tratamiento se realiza separadamente.

- Datos agregados. Se cede información agrupada o estadística sobre los datos originales (normalmente, el trabajo con este tipo de información ya no se considera como un tratamiento de datos personales, puesto que la información agregada no identifica a los afectados).
- Datos seudonimizados. Se ceden datos seudonimizados desde el tratamiento original (aunque hay datos personales, no hay identificación de los afectados). Debe existir una separación funcional y técnica entre investigadores y el equipo que realiza la seudonimización desde el tratamiento original, junto con los correspondientes compromisos de confidencialidad y medidas técnicas para evitar la reidentificación.
- Datos anonimizados. Se ceden datos anonimizados desde el tratamiento original (aunque hay datos personales, no hay identificación de los afectados). El tratamiento de datos correctamente anonimizados no se considera tratamiento de datos personales.

Como resumen, en esta fase inicial, se ha de constatar, por un lado, la fuente de los datos y, por otro, si la utilización de esos datos va a constituir un nuevo tratamiento de datos personales. Si se determina que no hay tratamiento de datos, el proceso termina. Si, por el contrario, se verifica que existen tratamientos, se pasa a la fase siguiente.

- **Fase 1. Identificación de los tratamientos.**

Una vez verificada la existencia de tratamientos de datos personales en el proyecto, es necesario identificarlos correctamente.

El investigador deberá reunir toda la información necesaria e identificar cada uno de los tratamientos de datos personales que serán aplicados en el proyecto, cumplimentando, en cada caso, la plantilla *Identificación de tratamiento de datos personales*[4], suministrada en el *Anexo 1* de esta memoria. Es necesario cumplimentar una plantilla por tratamiento (puede haber varios tratamientos distintos dentro de un mismo proyecto). Para obtener algunos de los datos requeridos, normalmente será necesario contactar con el DPD de la institución y con los responsables de las áreas técnicas encargados de implementar las posibles medidas de seguridad de las que se pudiera beneficiar el tratamiento.

[4] Para cumplimentar estas plantillas, aparte de consultar las instrucciones que se suministran, puede ser interesante para los investigadores revisar los conceptos plasmados en la *Guía para responsables de tratamiento*, elaborada por la AEPD y disponible en https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

De las plantillas cumplimentadas, se deben extraer datos fundamentales como:

- Identificación del proyecto de investigación.
- Descripción de las actividades de tratamiento de datos personales incluidas en el proyecto.
- Finalidad o finalidades del tratamiento o de los tratamientos.
- Identificación de la entidad o entidades responsables de los tratamientos de datos, junto con sus delegados de protección de datos (si tuvieran).
- Licitud del tratamiento. Vía o vías de legitimación de los tratamientos.
- Clasificación de las categorías de datos personales tratados e interesados afectados.
- Cesiones y transferencias internacionales de datos (si hubiera).
- Ciclos de vida y períodos de conservación de los datos.
- Tecnologías y roles de usuario implicados en la manipulación de los datos.
- Medidas de seguridad aplicadas.

Si el proyecto de investigación es finalmente validado y se va a llevar a cabo, la información obtenida con estas plantillas deberá comunicarse obligatoriamente al *Delegado de Protección de Datos*, o responsable equivalente, de las entidades participantes, con el objetivo de mantener el *Registro de Actividades de Tratamiento* (RAT) convenientemente actualizado (procedimiento obligatorio según las normativas vigentes).

- **Fase 2. Identificación de riesgos y clasificación del proyecto.**

Una vez identificados los tratamientos de datos personales, se han de documentar los riesgos asociados a cada uno de ellos. Cuando se habla de riesgos, en términos de protección de datos de carácter personal, se hace referencia a la posibilidad de que los intereses, derechos y libertades de los afectados se vean comprometidos debido a la exposición a amenazas relacionadas con la privacidad de sus datos. Al hablar de riesgo es necesario combinar la probabilidad de que se materialice una amenaza con las consecuencias negativas que este hecho pueda acarrear.

Según la *Guía práctica de Análisis de Riesgos en los tratamientos de datos personales sujetos al RGPD* (Agencia Española de Protección de Datos, 2018), las amenazas en los procesos de tratamiento de datos se pueden clasificar en tres tipos:

- Acceso no autorizado a los datos.
- Modificación no autorizada de los datos.
- Eliminación no autorizada de los datos.

En cuanto a los riesgos, la mencionada guía indica que es importante diferenciar entre:

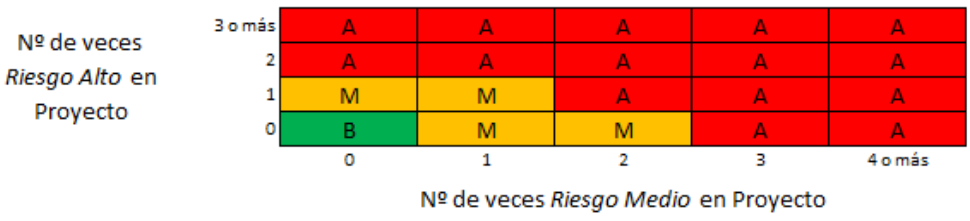
- Riesgos asociados a la protección de la información. Afectan a:
  - Integridad de los datos. Alteraciones o modificaciones no autorizadas de datos personales.
  - Disponibilidad de los datos. Borrados (totales o parciales) no autorizados de los datos o pérdidas en el acceso a los datos no autorizadas.
  - Confidencialidad de los datos. Accesos no autorizados a los datos personales.
- Riesgos asociados al cumplimiento de las obligaciones. Afectan a las garantías de:
  - Ejercicio de los derechos por parte de los interesados.
  - Cumplimiento de los *Principios relativos al tratamiento* (establecidos en el artículo 5 del RGPD y comentados en el apartado 2.3.1 de esta memoria) para cualquier tratamiento de datos.

Para poder identificar los riesgos asociados a un tratamiento, se analizarán las finalidades de dicho tratamiento comparadas con los daños y perjuicios sobre los intereses de los afectados, identificados en el Considerando 75 del RGPD y con las distintas amenazas documentadas en las guías relativas a gestión de riesgos en materia de datos personales publicadas por la AEPD.

En el *Anexo 2* de esta memoria se proporciona la plantilla *Identificación de riesgos en los tratamientos de datos personales*. Esta plantilla permite, además de ayudar al gestor a identificar los posibles riesgos en cada tratamiento, aplicar una clasificación del mismo en función del nivel global del riesgo. El tratamiento podrá ser de riesgo bajo (B), medio (M) o alto (A).

Del mismo modo, una vez clasificados los tratamientos, se podrá clasificar el proyecto de forma global, en función de los niveles de riesgo que tengan los diferentes tratamientos incluidos en el mismo. Para ello, bastará con hacer un recuento de los tratamientos con riesgo Medio y Alto, y aplicar la matriz de clasificación siguiente:

Figura 3. Clasificación del proyecto en base a los niveles de riesgo de los tratamientos.



Fuente: elaboración propia.

Una vez clasificados los tratamientos y el proyecto, los investigadores deberán actuar en consecuencia. En los casos en que se detecten proyectos de riesgo medio y alto, será obligatoria y fundamental la colaboración de los *Delegados de Protección de Datos* de las entidades responsables de los tratamientos, con quienes se valorará la posible realización de *Evaluaciones de Impacto en Protección de Datos* (EIPD) y con quien se coordinará la toma de medidas técnicas y organizativas adecuadas para evitar la materialización de las amenazas detectadas.

- **Fase 3. Entrega de información al interesado y obtención del consentimiento.**

En todos aquellos proyectos que requieran recabar datos directamente de los interesados o afectados, el responsable deberá:

- Aportar a los interesados toda la información exigida sobre el proceso.
- Construir un correcto sistema de obtención de consentimientos.

Desde el punto de vista de la normativa de protección de datos, es fundamental comunicar al interesado la información adecuada sobre el tratamiento. Además, el hecho de que el interesado esté bien informado, será importante para que éste pueda decidir si consiente o no dicho tratamiento. El *Grupo de Trabajo del Artículo 29* (ahora *Comité Europeo de Protección de Datos*) consideró que, para que un consentimiento sea válido, se requiere, al menos, que el responsable proporcione la siguiente información al interesado (Grupo de Trabajo del Artículo 29 sobre Protección de Datos, 2018):

- Identidad del responsable del tratamiento.
- Finalidad de cada una de las operaciones del tratamiento para las que se solicita el consentimiento.
- Identificar las tipologías de datos que van a recogerse y utilizarse en el tratamiento.
- Expresar la existencia del derecho a retirar el consentimiento por parte del interesado.
- Incluir información sobre la utilización de los datos obtenidos para la toma de decisiones automatizadas, cuando sea el caso.
- Incluir información sobre los posibles riesgos si se producen transferencias de datos a países sobre los que la Comisión Europea no haya emitido una decisión de adecuación, o sobre los que no se cuenta con garantías adecuadas.

Además, tal y como se indica en *Guía para el cumplimiento del deber de informar* (Agencia Española de Protección de Datos, 2017), el RGPD incluye nuevas obligaciones en el deber de información. La guía agrupa la información a aportar por el responsable en una serie de epígrafes cuyos datos se pueden presentar en dos capas o niveles. La primera de ellas tiene un carácter de resumen y la segunda debe aportar un adecuado nivel de detalle.

Figura 4. Información por capas.

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

Fuente: Guía para el cumplimiento del deber de informar (Agencia Española de Protección de Datos, 2017)

Según la mencionada guía, la información básica de primera capa debe situarse en los formularios de solicitud, ya sean electrónicos o en papel, o bien debe estar presente en cualquier solicitud mediante entrevista telefónica. En esta primera capa deberá existir la posibilidad de acceder a la segunda.

La información de segunda capa debe completar, con todos los detalles, la información de primera capa, incluyendo todas las características exigidas por el RGPD. Se puede proporcionar en papel (documentos anexos o en el reverso del formulario), en una página web (la opción más interesante) o mediante una locución telefónica que incluya todos los datos.

Por otro lado, el consentimiento es una de las bases jurídicas más habituales en el área de la investigación para permitir al responsable el tratamiento de los datos del interesado. Será necesario, además, tener especial atención con la gestión del consentimiento en aquellos proyectos cuyo trabajo se realiza con datos especialmente protegidos.

Como ya se ha comentado anteriormente, el RGPD ha especificado, en cuanto al consentimiento, que:

- Debe ser explícito y el responsable debe poder demostrar que el titular de los datos lo prestó.
- Debe existir un consentimiento para cada finalidad del tratamiento.
- Debe poder ser revocado en cualquier momento por parte de los afectados.

En la disposición adicional decimoséptima de la LOPDGDD se recogen algunos criterios que afectan a la licitud (consentimiento) y a los derechos del interesado en tratamientos relacionados con la investigación que suponen importantes excepciones a las normas generales. Permiten realizar tratamientos sin consentimiento a las autoridades sanitarias e instituciones públicas en procesos de investigación ejecutados en situaciones de especial gravedad y la reutilización sin consentimiento de datos personales para investigaciones en áreas relacionadas con las del tratamiento inicial.

Por otro lado, la referencia fundamental en proyectos de investigación del área de la salud es el *Consentimiento Informado*. La AEMPS proporciona una serie de instrucciones para la correcta elaboración de un modelo de hoja de información al paciente (HIP) y consentimiento informado (CI). Los proyectos cuyo objetivo es la investigación clínica con medicamentos o productos sanitarios, deberán atenerse a las mencionadas instrucciones[5].

En el *Anexo 3* de esta memoria, se proporciona una plantilla que, teniendo en cuenta todas las indicaciones mencionadas, recoge un *Documento estándar de Consentimiento Informado* aplicable de forma genérica a cualquier proyecto de investigación, exceptuando los referenciados en el párrafo anterior, que deberán utilizar el mencionado modelo de la AEMPS. Esta plantilla deberá cumplimentarse y ajustarse a las características concretas de cada proyecto y se proporcionará a todas aquellas personas que quieran participar en el mismo.

- **Fase 4. Implementación del ejercicio de derechos por parte de los interesados.**

Tal y como se ha comentado en el apartado 2.3.1 de esta memoria, el RGPD (y, por ende, la LOPDGDD) ha revisado y reforzado los derechos de los interesados en cualquier tratamiento de datos personales. Es muy importante que los responsables de los tratamientos adopten las medidas necesarias para permitir el acceso de los interesados a estos derechos.

La implementación de estas medidas deberá ser realizada por los responsables del proyecto de investigación, pero es fundamental que sean coordinadas con los DPD de las entidades responsables, de forma que todas las medidas queden correctamente documentadas en las instituciones responsables (principio de *responsabilidad proactiva*).

Es importante indicar que:

- Los derechos del interesado se deben preservar tanto en los tratamientos en los que se recaban los datos directamente del interesado como en aquellos en los que los datos han sido cedidos desde un tratamiento anterior.

[5] Instrucciones disponibles en los anexos VIIIA, VIIIB y VIIIC de la AEMPS, publicados en la página https://www.aemps.gob.es/investigacionClinica/medicamentos/anexos-instrucciones-AEMPS-realiza-EC.htm

- En el caso de personas fallecidas, la gestión de los derechos, podrá ser llevada a cabo por familiares, o herederos (art. 3 LOPDGDD).

Seguidamente, se revisan los derechos y se realizan propuestas de implementación de los mismos en un entorno de investigación universitaria.

1. *Información*.

El derecho a la información por parte de los interesados debe estar cubierto desde la primera interacción de los mismos con la gestión del tratamiento. En la fase 3 de esta metodología se han revisado algunas de las claves en cuanto a la obligación de proporcionar información al interesado de forma previa a que éste decida sobre su consentimiento (aplicable a los casos en los que se recaban los datos directamente del interesado). Dicha información, que inicialmente se ha proporcionado desde la plataforma sobre la que se solicita el consentimiento, deberá estar también íntegramente recogida en una ubicación pública permanente, a la que se pueda acceder de forma cómoda en cualquier momento.

La propuesta de esta metodología para lograr el objetivo de la información es habilitar una web pública para cada proyecto de investigación (gestionada por el responsable –universidad o investigadores- o por los posibles encargados del tratamiento). En ella, se deberá incorporar, al menos, la siguiente información:

- Datos generales sobre el proyecto de investigación. Nombre del proyecto, área de estudio, universidades participantes, investigadores participantes, objetivos, metodologías, alcances, etc.
- Identificación de todos los tratamientos de datos personales desarrollados. Para cada tratamiento, se ha de añadir toda la información obligatoria especificada en el RGPD. Es necesario diferenciar dos casos:
    - Tratamientos en los que los datos se obtienen directamente del interesado. Es necesario publicar la información identificada en el artículo 13 del RGPD.
    - Tratamientos en los que los datos se obtienen de tratamientos previos y no directamente del interesado. Es necesario publicar la información identificada en el artículo 14 del RGPD. Este aspecto es muy importante, ya que es fundamental informar a los afectados sobre el origen de los datos, sobre todo cuando éstos datos no se les han recabado directamente a ellos, sino que tienen su origen en una cesión desde otro tratamiento.

Como medida recomendable (aplicable siempre que el consumo de recursos para llevarla a cabo sea razonable), se propone realizar una comunicación individualizada (vía e-mail, llamada telefónica o similar) a todos los afectados en aquellos casos en los que el proyecto

de investigación utilice datos personales no obtenidos directamente de los afectados, sino de otros tratamientos previos que dispongan de legitimación para ceder los mismos a este tipo de proyectos.

2. *Acceso*.

El derecho de acceso se refiere, no sólo a que el interesado pueda conocer toda la información disponible sobre el tratamiento (reflejada en el punto anterior), sino a también a que éste pueda revisar todos los datos personales que, sobre su persona, obren en poder de los responsables (o encargados, en su caso) del tratamiento (el artículo 15 del RGPD define las obligaciones en este sentido).

La web informativa del proyecto cubriría la primera parte de este derecho, pero implementar el acceso remoto automatizado a la información personal de cada interesado es una tarea mucho más compleja. En la mayoría de los casos, implementar un acceso remoto privado, autenticado y seguro (por ejemplo, de tipo web) a los datos sería suficiente (así lo reconoce la LOPDGDD en su artículo 13), pero requiere una cantidad de recursos muy elevada y es probable que muchos responsables de los proyectos no puedan asumir los costes de esta publicación (salvo en aquellos casos en los que los datos tratados deban estar completamente automatizados, publicados y disponibles bajo este tipo de accesos remotos seguros porque el estudio así lo requiera).

La recomendación de esta metodología para implementar el ejercicio de este derecho (si no fuera posible el mencionado acceso automatizado) es la incorporación a la web informativa del proyecto de un sistema de formularios en los que los interesados puedan solicitar el acceso a sus datos y una copia de los mismos. Dichos formularios (implementados bajo un sistema seguro, atendiendo a los estándares actuales aplicables a los sistemas de información), deberán incluir información obligatoria que será almacenada en una base de datos para poder consultar todas las actividades en cualquier momento. Datos a incluir:

- Identificación del interesado con, al menos, dos factores. Antes de comunicar los datos, el responsable deberá comprobar la identidad del solicitante.
- Fecha de solicitud.
- Motivo de la solicitud.
- Categorías de datos concretas a los que se solicita acceso.
- Incluir un sistema de validación, tipo *captcha*, para impedir consultas automatizadas fraudulentas.

Los responsables del proyecto de investigación, deberán atender estas peticiones, teniendo en cuenta que:

- La copia de los datos proporcionada al interesado deberá contener única y exclusivamente información sobre el interesado solicitante.
- La copia se deberá proporcionar, en la medida de lo posible, en formato electrónico.
- Plazo máximo para entregar la copia: 1 mes desde la solicitud, aunque se puede prorrogar a 2 meses si las solicitudes son complejas.
- El procedimiento debe ser gratuito para el interesado, aunque en casos extremos (peticiones infundadas, excesivas o repetitivas) se podrán aplicar costes razonables.
- Si la solicitud de acceso se deniega, se deberá comunicar al interesado en un plazo máximo de 1 mes desde la solicitud, incluyendo las razones e información sobre la posibilidad de presentar reclamación ante las autoridades de control competentes.
- La entrega de los datos se realizará, preferiblemente, a través de medios electrónicos y, en todo caso, incluyendo sistemas que permitan guardar y acreditar constancia de dicha entrega (modo, contenido y fecha).

3. *Rectificación*.

El derecho de rectificación permite al interesado solicitar la corrección de la copia de sus datos personales que obra en poder del responsable, cuando éstos contengan datos incorrectos, inexactos o incompletos.

El modo propuesto para que los interesados puedan solicitar esta corrección es un sistema de formularios similar al propuesto en el apartado anterior. En este caso, se implementará con los siguientes datos:

- Identificación del interesado con, al menos, dos factores. Antes de comunicar los datos, el responsable deberá comprobar la identidad del solicitante.
- Fecha de solicitud.
- Motivo de la solicitud.
- Datos concretos sobre los que se solicita la modificación. Indicar la categoría y el dato actualizado (en algunos casos, incluso se podría requerir documentación justificativa).
- Incluir un sistema de validación, tipo *captcha*, para impedir consultas automatizadas fraudulentas.

El responsable deberá contestar a la solicitud, preferentemente por medios electrónicos, indicando si es aceptada o no y, en caso positivo, la fecha en la que la modificación de los datos será operativa. La contestación, igual que en el caso anterior, deberá quedar

correctamente acreditada y almacenada (con todos los datos que incluya y la fecha de su envío). Los plazos y condiciones son similares a los expuestos en el apartado anterior.

4. *Oposición*.

El derecho de oposición recoge la posibilidad de que un afectado, en cualquier momento, cambie de opinión y deniegue su permiso (es decir, anule su consentimiento) para que sus datos personales sean tratados en un proyecto de investigación activo. El derecho de oposición supone la detención del tratamiento, pero, por defecto, no tiene por qué suponer la eliminación de los mismos por parte del responsable.

En tratamientos de datos generales, este derecho es fundamental y se debe atender en un porcentaje muy alto de situaciones. Sin embargo, en el caso de la investigación científica, histórica o estadística, el responsable tendrá la opción de desestimar la solicitud de oposición en aquellos casos en los que puedan acreditar, debidamente, las siguientes dos razones:

- El tratamiento de datos personales afectado es necesario para el cumplimiento de una misión de interés público.
- Los datos concretos del interesado son fundamentales para el tratamiento afectado.

La implementación de la medida que permita ejercer este derecho a los interesados se llevará a cabo, nuevamente, con un sistema de formularios publicados en la web del proyecto, de un modo análogo a los anteriores. En este caso, con los siguientes datos:

- Identificación del interesado con, al menos, dos factores. Antes de comunicar los datos, el responsable deberá comprobar la identidad del solicitante.
- Fecha de solicitud.
- Motivo de la solicitud.
- Categorías de datos concretos sobre los que se solicita la oposición.
- Incluir un sistema de validación, tipo *captcha*, para impedir consultas automatizadas fraudulentas.

El responsable deberá contestar a la solicitud, preferentemente por medios electrónicos, indicando si es aceptada o no y, en caso positivo, la fecha en la que el cese del tratamiento será operativo. Además, el responsable deberá informar que el derecho de oposición no elimina los datos y que, si el interesado desea este extremo, deberá cumplimentar la correspondiente solicitud de supresión (se revisa en el apartado siguiente). La contestación, igual que en los casos anteriores, deberá quedar correctamente acreditada y almacenada (con todos los datos que incluya y la fecha de su envío). Los plazos y condiciones son similares a los expuestos en los formularios anteriores.

En los casos en que el derecho de oposición se apruebe, es recomendable la extracción de la información afectada de la base de datos del tratamiento y su almacenado en un sistema de información separado, totalmente fuera del alcance de dicho tratamiento.

5. *Supresión*.

El derecho de supresión implica la eliminación definitiva de los datos personales del afectado que estén en poder del responsable del tratamiento. El artículo 17 del RGPD enumera las circunstancias en las que el interesado podrá solicitar la supresión de sus datos personales.

En el ámbito de la investigación universitaria, esta figura puede estar encajada en supuestos como, por ejemplo, los siguientes:

- Casos en los que el afectado ha solicitado la oposición
- Casos en los que los proyectos ya no están activos y el afectado quiere que sus datos sean eliminados.
- Casos en los que el consentimiento no fuera válido.
- Etc.

La vía de ejercicio del derecho se implementará, una vez más, con un sistema de formularios publicados en la web del proyecto, de un modo análogo a los anteriores. En este caso, deben incluir los siguientes datos:

- Identificación del interesado con, al menos, dos factores. Antes de comunicar los datos, el responsable deberá comprobar la identidad del solicitante.
- Fecha de solicitud.
- Motivo de la solicitud.
- Categorías de datos concretos sobre los que se solicita la supresión.
- Incluir un sistema de validación, tipo *captcha*, para impedir consultas automatizadas fraudulentas.

El responsable deberá contestar a la solicitud, preferentemente por medios electrónicos, indicando si es aceptada o no y, en caso positivo, la fecha en la que la eliminación de los datos será operativa. La contestación, igual que en los casos anteriores, deberá quedar correctamente acreditada y almacenada (con todos los datos que incluya y la fecha de su envío). Los plazos y condiciones son similares a los expuestos en los formularios anteriores.

6. *Limitación del tratamiento*.

El derecho de limitación del tratamiento supone la reducción (temporal o definitiva) del tratamiento a la mera conservación de los datos para la formulación, ejercicio o defensa de

reclamaciones; para proteger los derechos de otra persona o por razones de interés público. Es decir, el responsable podrá conservar los datos, pero no procesarlos bajo el tratamiento inicial.

Según el artículo 18 del RGPD, los supuestos de limitación se aplican, normalmente, cuando existe alguna circunstancia por la que el interesado requiere modificaciones que afectan sensiblemente al tratamiento (corrección de datos inexactos, tratamiento ilícito, oposición, etc.)

Una vez más, se podrá implementar el ejercicio de este derecho con un sistema de formularios publicados en la web del proyecto, de un modo análogo a los anteriores. En este caso, deben incluir los siguientes datos:

- Identificación del interesado con, al menos, dos factores. Antes de comunicar los datos, el responsable deberá comprobar la identidad del solicitante.
- Fecha de solicitud.
- Motivo de la solicitud.
- Categorías de datos concretos sobre los que se solicita la limitación.
- Incluir un sistema de validación, tipo *captcha*, para impedir consultas automatizadas fraudulentas.

El responsable deberá contestar a la solicitud, preferentemente por medios electrónicos, indicando si es aceptada o no y, en caso positivo, la fecha en la que la limitación del tratamiento será operativa. La contestación, igual que en los casos anteriores, deberá quedar correctamente acreditada y almacenada (con todos los datos que incluya y la fecha de su envío). Los plazos y condiciones son similares a los expuestos en los formularios anteriores.

En los casos en que el derecho de limitación se apruebe, es recomendable la extracción de la información afectada de la base de datos del tratamiento y su almacenado en un sistema de información separado, totalmente fuera del alcance de dicho tratamiento.

7. *Oposición a ser objeto de decisiones individuales automatizadas*.

Este derecho, regulado en el artículo 22 del RGPD, habilita la oposición de un interesado a que se vea afectado por decisiones con efectos jurídicos o que le afecten significativamente (incluida la generación automatizada de perfiles) y que se toman en base a tratamientos automatizados, salvo que dichas decisiones sean necesarias para la ejecución de un contrato, estén habilitadas por un consentimiento explícito del interesado o estén autorizadas por el derecho comunitario.

Si el proyecto de investigación incluye tratamientos de este tipo, será fundamental habilitar la posibilidad de que el interesado consienta este aspecto en el *Documento de Consentimiento Informado* (apartado *Consentimientos*).

Por otro lado, la implementación para poder ejercer este derecho de oposición (que, como cualquiera de los anteriores, se podría ejecutar en cualquier momento) se llevará a cabo con el correspondiente formulario publicado en la web del proyecto, de un modo análogo a los anteriores. En este caso, deben incluir los siguientes datos:

- Identificación del interesado con, al menos, dos factores. Antes de comunicar los datos, el responsable deberá comprobar la identidad del solicitante.
- Fecha de solicitud.
- Motivo de la solicitud.
- Procedimientos concretos sobre los que se solicita la anulación de las tomas de decisiones automatizadas o generación de perfiles automatizados.
- Incluir un sistema de validación, tipo *captcha*, para impedir consultas automatizadas fraudulentas.

El responsable deberá contestar a la solicitud, preferentemente por medios electrónicos, indicando si es aceptada o no y, en caso positivo, la fecha en la que la modificación del tratamiento será operativa. La contestación, igual que en los casos anteriores, deberá quedar correctamente acreditada y almacenada (con todos los datos que incluya y la fecha de su envío). Los plazos y condiciones son similares a los expuestos en los formularios anteriores.

En los casos en que esta solicitud se apruebe, el responsable debe analizar los efectos sobre el tratamiento concreto. Si todo el tratamiento se basa en este tipo de decisiones o automatizaciones, lo recomendable sería excluir del estudio todos los datos del afectado (hecho que se debería comunicar a dicho interesado). Si el tratamiento sobre los datos sigue siendo posible aun anulando los procedimientos afectados por este derecho de anulación, se seguirá llevando a cabo con las modificaciones pertinentes.

8. *Portabilidad*.

El derecho a la portabilidad, definido en el artículo 20 del RGPD, implica que los datos puedan, ser transferidos de un responsable a otro, bajo la solicitud del interesado, sin que éste tenga que intervenir en el proceso. Para ello, es necesario que la información esté automatizada y formateada bajo un esquema de utilización común. Esto no siempre es técnicamente posible y, por lo tanto, este derecho no se puede garantizar en todas las ocasiones.

Es importante indicar que el derecho de portabilidad sólo se aplicará sobre los datos que el interesado haya aportado directamente al responsable, es decir, no será aplicable a la información que el responsable del tratamiento haya inferido o deducido sobre el interesado, o a cualquiera de los resultados generados por la aplicación del tratamiento de datos original.

Este derecho está pensado para ámbitos como la prestación de servicios electrónicos (correo electrónico, telefonía, etc.), servicios bancarios, etc. y, al menos de momento, no es habitual en los entornos de investigación universitaria. Sin embargo, con el aumento de la concienciación de los ciudadanos sobre la importancia de la investigación, por ejemplo, en los campos de la biotecnología, genética, etc., podría darse el caso que los afectados pudieran solicitar la portabilidad de sus datos de un proyecto de investigación a otro.

Para cubrir este tipo de casos, la recomendación es implementar el ejercicio del derecho mediante otro formulario similar a los anteriores. Los datos a cubrir son:

- Identificación del interesado con, al menos, dos factores. Antes de comunicar los datos, el responsable deberá comprobar la identidad del solicitante.
- Fecha de solicitud.
- Motivo de la solicitud.
- Categorías de datos concretos sobre los que se solicita la portabilidad.
- Formato preferido para transferir los datos.
- Incluir un sistema de validación, tipo *captcha*, para impedir consultas automatizadas fraudulentas.

Los responsables técnicos del proyecto deberán estudiar, en cada caso, la viabilidad de la exportación de los datos en el formato solicitado. En los casos en que sea técnicamente posible y la petición se apruebe, será necesario realizar una extracción manual de los datos afectados, la conversión al formato solicitado y el envío seguro de los mismos (preferentemente por medios electrónicos).

El responsable deberá contestar a la solicitud, preferentemente por medios electrónicos, indicando si es aceptada o no y, en caso positivo, la fecha en la que el proceso de portabilidad podrá ser realizado. Además, el responsable deberá informar que el derecho de portabilidad no implica la detención del tratamiento original ni la eliminación de los datos (considerando 68 del RGPD) y que, si el interesado desea estos extremos, deberá cumplimentar las correspondientes solicitudes de oposición y supresión. La contestación, igual que en los casos anteriores, deberá quedar correctamente acreditada y almacenada (con todos los datos que incluya y la fecha de su envío). Los plazos y condiciones son similares a los expuestos en los formularios anteriores.

- **Fase 5. Aplicación de medidas de seguridad (investigadores y universidad).**

Tal y como se ha dejado patente a lo largo de esta memoria, la ejecución de tratamientos de datos personales es una práctica que conlleva determinados riesgos. Para lograr el objetivo de preservar los derechos y libertades de las personas físicas, será necesario minimizar esos riesgos aplicando los controles o medidas de seguridad adecuados.

Evidentemente, no todos los tratamientos de datos personales conllevan el mismo nivel de riesgo y, por lo tanto, en todos los casos no es necesario aplicar las mismas medidas de seguridad. En la legislación anterior, existían catálogos de medidas de seguridad aplicables en función del nivel de sensibilidad de la información a proteger. Con el RGPD, esta orientación cambia y se propone que el responsable será el que, desde el primer momento, valore el riesgo y las medidas a aplicar, teniendo en cuenta los principios fundamentales, tanto de *Protección de datos desde el diseño y por defecto* como de *Responsabilidad proactiva*. Por este motivo, sólo se habla, en general, de aplicar medidas técnicas y organizativas adecuadas, indicando algunos ejemplos de las mismas (seudonimización, minimización de datos, etc.).

La elección de medidas a aplicar es un proceso para el que hay que contar con la asesoría del *Delegado de Protección de Datos* de las instituciones responsables. Esta figura deberá conocer las medidas ya disponibles, de forma global, en dichas instituciones y podrá asesorar, de acuerdo con las finalidades de los tratamientos y recursos disponibles para cada proyecto, sobre las medidas a aplicar/reforzar en cada caso concreto.

Existen diversos estándares que recogen catálogos de amenazas/soluciones aplicables en procesos de análisis de riesgos. Para confeccionar este documento, se han estudiado tres fuentes:

- *Metodología de Análisis y gestión de Riesgos de los Sistemas de Información*. *MAGERIT* (versión 3.0)[6], publicada por el *Ministerio de Hacienda y Administraciones públicas*. Apartados *5. Amenazas* y *6. Salvaguardas*. Describe un catálogo público de amenazas y salvaguardas general, aplicable a cualquier análisis de riesgos, no sólo a protección de datos personales. La detección de las amenazas descritas y la aplicación de las medidas propuestas puede ser compleja, por lo que su utilización deberá ser supervisada por expertos en seguridad.
- Norma *ISO/IEC 27002*. Estándar de seguridad publicado por la *Organización Internacional de Normalización* (ISO). Describe un catálogo de controles para implementar un Sistema de Gestión de la Seguridad de la Información y su

[6] Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

implantación. No es un estándar público, por lo que, en caso de aplicarlo, será necesario adquirir la norma correspondiente. La aplicación de las medidas propuestas puede ser compleja, por lo que su utilización deberá ser supervisada por expertos en seguridad.

- *Guía práctica para las evaluaciones de impacto en la protección de datos personales*, publicada por la AEPD. Apartados *5.5 Anexo V: Catálogo de amenazas* y *5.6 Anexo VI: Catálogo de amenazas y posibles soluciones.* Este catálogo se centra en riesgos y controles relacionados con los tratamientos de datos personales, por lo que es uno de los más adecuados para ser tenido en cuenta en el contexto de este estudio.

Tras el estudio de las mencionadas fuentes y, como referencia para el uso por los responsables de proyectos de investigación, se aporta el *Anexo 4* de esta memoria, en el que se incluye el *Catálogo general de amenazas y posibles soluciones, aplicable a los tratamientos de datos personales*, elaborado a partir de los apartados *5.5 Anexo V: Catálogo de amenazas* y *5.6 Anexo VI: Catálogo de amenazas y posibles soluciones* de la *Guía práctica para las evaluaciones de impacto en la protección de datos personales* (Agencia Española de Protección de Datos, 2018). Se trata de un catálogo general, aplicable a cualquier tipo de tratamiento de datos, sobre el que se han añadido algunas medidas específicas para los tratamientos de datos incluidos en proyectos de investigación universitarios. Se recomienda su uso teniendo en cuenta que:

- En los casos de proyectos que incluyan tratamientos de datos personales sensibles, será necesario profundizar en la complejidad de las medidas concretas aplicables. Es fundamental contar con la colaboración del *Delegado de Protección de Datos* y los responsables de seguridad de las instituciones participantes.
- Existen medidas que, por su complejidad, deben ser implementadas a nivel de institución y no a nivel de proyecto de investigación.

- **Fase 6. Aplicación de anonimización y seudonimización.**

Tanto la *anonimización* como la *seudonimización* (conceptos definidos en el apartado 2.1 de esta memoria) son medidas de seguridad que forman parte de las prácticas fundamentales en muchos proyectos de investigación y, dada la complejidad en su aplicación, requieren de un estudio en profundidad.

El considerando 156 del RGPD establece una clara preferencia por la aplicación de procesos de anonimización o seudonimización en la fase de publicación de resultados obtenidos en el proceso de investigación.

La decisión sobre si estas técnicas son adecuadas para ser aplicadas o no, dependerá del tipo de proyecto y, por supuesto, de los tipos de datos que maneje y de los recursos disponibles. Pero, teniendo en cuenta que estas técnicas siempre aportan un mayor nivel de seguridad a los tratamientos de datos personales y a la protección de los derechos del interesado, se recomienda valorar, en todos los casos, la idoneidad de su aplicación.

Definir plantillas estándar que habiliten su aplicación de forma generalizada es muy complicado, por lo que en esta memoria se propone un esquema de trabajo que requerirá un estudio específico adaptado a cada caso concreto. Se requerirá el apoyo del *Delegado de Protección de Datos* de la institución responsable.

Anonimización.

Los procesos de anonimización, que, como ya se ha comentado, desactivan la característica de 'tratamiento de datos personales' a los datos así tratados, son posibles en aquellos casos en los que se pueda prescindir de todos los datos identificativos de los sujetos objeto de estudio, es decir, en todos aquellos casos en los que los que no se estudien los propios datos identificativos (por ejemplo, en estudios sobre software de reconocimiento facial) y en los que no sea necesario mantener identificados a los afectados (por ejemplo, para establecer algún tipo de comunicación posterior con ellos).

Según la guía *Orientaciones y garantías en los procedimientos de anonimización de datos personales* (Agencia Española de Protección de Datos, 2016), son muchas las variables a tener en cuenta para aplicar correctamente las técnicas de anonimización. En la metodología propuesta en esta memoria, se resumen y adaptan las más oportunas para aplicar en proyectos de investigación universitaria.

Lo primero que hay que tener en cuenta es que existen datos de identificación directa (aquellos que, por si mismos, identifican a la persona) y datos de identificación indirecta (aquellos que, por si mismos, no identifican a la persona pero que, combinados con otros, pueden llegar a hacerlo). Ejemplos:

- Datos de identificación directa: nombre y apellidos, DNI, fotografía del rostro, etc.
- Datos de identificación indirecta: hay ciertas combinaciones de datos (que individualmente no son de identificación directa), como, por ejemplo, la conjunción de sexo, lugar de nacimiento, lugar de residencia, edad y datos de afección de una determinada enfermedad, que pueden llegar a permitir la identificación indirecta de una persona.

Un proceso de anonimización adecuado debe identificar todos los datos de identificación directa y realizar un estudio sobre los posibles datos de identificación indirecta (tanto los disponibles en el propio tratamiento como los que se podrían encontrar y combinar en fuentes externas, como búsquedas por Internet). Dada la cantidad de variables que pueden influir, garantizar el 100% de irreversibilidad en los procesos de anonimización es muy complicado en algunos casos.

En el entorno de la investigación, los procesos de anonimización de los datos se llevan a cabo en dos circunstancias:

- Datos obtenidos directamente de los afectados por los investigadores. La anonimización se llevará a cabo, normalmente, inmediatamente antes de procesos como la publicación de los resultados de la investigación o cuando se quieran preparar los datos para una conservación segura a largo plazo. La anonimización será ejecutada por los propios investigadores que han recogido los datos.
- Datos obtenidos de tratamientos previos (por ejemplo, hospitales que ceden datos anónimos a un grupo de investigación). La anonimización debe ser previa a la cesión y realizada por los responsables de los tratamientos originales.

Las recomendaciones para ejecutar un correcto proceso de anonimización en el ámbito de la investigación universitaria (basadas en la mencionada guía de la AEPD y cuya consulta es recomendada para obtener información avanzada sobre los pasos a realizar en cada fase), son las siguientes:

1. Definir un equipo de trabajo para llevar a cabo el proceso. Deberán participar todas las figuras relacionadas del responsable (responsable tratamiento original, DPD, equipo de seguridad de la información, equipo de investigadores, etc.) y, si es posible, un representante del destinatario de la información (en su caso).
2. Evaluar los posibles riesgos de la reidentificación de las personas afectadas, para poder gestionarlos con las correspondientes medidas técnicas, organizativas o de otro tipo.
3. Definir la finalidad del proceso y los objetivos a perseguir con la anonimización de la información afectada. Estudiar la viabilidad del mismo.
4. Definir las variables de identificación, directas e indirectas, afectadas en el proceso. Reducir al máximo las que permitan la reidentificación de las personas.
5. Estudiar los casos de datos especiales, como los registros de voz, registros de imagen (fotografías o vídeos) y los datos biométricos. En algunos casos, como los datos biométricos, la finalidad de la información puede ser un límite a la anonimización de la misma, por lo que, en algunos casos, se deberán aplicar excepciones (que serán contempladas en posibles EIPD).

6. Existen dos familias de técnicas de anonimización: aleatorización (modifica los datos con el objetivo de tratar de eliminar el vínculo existente entre ellos y la persona) y generalización (trata de diluir los atributos de los interesados modificando las escalas u órdenes de magnitud, por ejemplo, sustituyendo ciudad por región o semana por mes). Dentro de ellas, hay que seleccionar las técnicas de anonimización adecuadas. Las más empleadas son[7]:
    a. Algoritmos Hash. Combinados, en ciertos casos, con códigos de autentificación de mensajes criptográficos, que mezclan hash con claves secretas (ejemplo: HMAC).
    b. Algoritmos de cifrado, sobre todo los que presentan propiedades homomórficas[8].
    c. Firma electrónica y sellos de tiempo. Ayudan a identificar al anonimizador y la fecha y hora de la anonimización.
    d. Agregación de datos. Ejecución de operaciones sistemáticas sobre datos específicos para que las cifras globales resultantes no revelen información sobre los casos específicos.
    e. Reducción de datos. Eliminación de datos originales (sobre todo los atributos obvios y los cuasi identificadores) para disminuir el detalle en datos que no tengan relevancia para el resultado final.
    f. Capas de anonimización. Se pueden llevar a cabo sucesivos procesos de anonimización (tanto por el responsable inicial como por el destinatario, o en distintos departamentos a los que llegue la información).
7. Realizar la anonimización, aplicando la técnica más adecuada en función de las variables identificadas.
8. Formación a las personas que trabajarán con los datos anonimizados. Se debe formar, entre otras cosas, sobre las medidas de seguridad y de control aplicables, políticas de uso de la información anonimizada y obligaciones en caso de producirse casos de identificación en los datos anonimizados.
9. Establecer garantías jurídicas (acuerdos de confidencialidad, compromisos para mantener la anonimización, auditorías, etc.) y documentar el proceso.

[7] Más información en el siguiente artículo del Grupo de trabajo del artículo 29 sobre Técnicas de Anonimización y Seudonimización: https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf
[8] Cifrado homomórfico. Bajo ciertas condiciones, permite ejecutar operaciones algebraicas sobre el dato cifrado, de forma que los resultados de las mismas serían similares a los obtenidos de haberse ejecutado las mismas operaciones sobre los datos sin cifrar.

Seudonimización.

La finalidad última de la seudonimización es similar a la de la anonimización, es decir, evitar que el interesado sea identificado en la medida de lo posible. Sin embargo, el resultado y los métodos que emplea son distintos, ya que, en este caso, siempre es posible la reidentificación mediante la aplicación inversa del algoritmo de seudonimización. El procedimiento habitual es sustituir un atributo identificativo por otro que no permita la identificación directa y luego guardar, de forma segura y separada, el procedimiento y claves de conversión. Por este motivo, es fundamental proteger la información adicional que permite la reidentificación del interesado. La seudonimización no es un tipo de anonimización.

Los tipos más utilizados de seudonimización son los siguientes:

- Sustitución de cifras y códigos por palabras.
- Codificación o encriptado de la información. Se trata de una de las medidas más seguras y, por tanto, aconsejables para su aplicación. Las técnicas más habituales son:
    - Aplicación de técnicas de cifrado seguras sobre los atributos identificativos.
    - Aplicación de técnicas de obtención de *hash*[9] sobre los atributos identificativos.
    - Combinación de cifrado y hash.
- Introducción de números aleatorios sin relación con el original para identificar la información.
- Intercambio de números aleatorios por un conjunto de datos.
- Etc.

Se trata de una medida de seguridad más para reducir el riesgo del tratamiento. Puede realizarse tanto por el responsable como por los posibles encargados del tratamiento.

En el caso de proyectos de investigación con datos seudonimizados será fundamental:

- Aplicar las medidas técnicas y organizativas adecuadas para mantener la confidencialidad, integridad y disponibilidad de las claves para re-identificar la información (por ejemplo, cifrar el fichero que contiene las claves, guardarlo en un sistema de almacenamiento seguro y restringir el acceso al mismo).
- En los casos de cesión de datos (a nuevos proyectos de investigación, por ejemplo) se deberá estudiar, para cada caso, si es pertinente la entrega de los datos personales seudonimizados o no. En el caso de producirse una entrega de datos seudonimizados

[9] Más información en el siguiente artículo de la AEPD sobre la utilización del HASH como técnica de seudonimización: https://www.aepd.es/sites/default/files/2019-11/estudio-hash-anonimidad.pdf

sin las correspondientes claves de reidentificación, se tratará de una entrega de datos anónimos y, por lo tanto, el nuevo tratamiento no se considerará como un tratamiento de datos de carácter personal afectado por RGPD y LOPDGDD.

- En investigación con datos de salud, la seudonimización es fundamental y, en muchos casos, obligatoria frente a la anonimización. Ambas técnicas reducen igualmente el riesgo en la operativa del tratamiento, pero en este tipo de investigación puede ser clave la aplicación de la seudonimización frente a la anonimización. Esto es porque, en muchas ocasiones, es necesario re-identificar a los afectados, por ejemplo, para realizar comunicaciones relacionadas con los resultados obtenidos.

- **Fase 7. Análisis de las implicaciones de los tratamientos.**

Como última fase de la metodología y, tras recorrer el camino propuesto por ella, los responsables del proyecto deberían haber captado una idea, ya bastante amplia, de los tratamientos que se llevan a cabo en el mismo y las implicaciones que tienen.

En esta fase, se relacional los puntos clave de gestión de los tratamientos y las implicaciones para con las instituciones responsables:

1. *Comunicación de existencia de tratamientos de datos personales al DPD*.

Siempre que se compruebe que existe un tratamiento de datos de carácter personal, se deberá comunicar este hecho al DPD de la institución responsable. En la fase 0 de la metodología se determinará la existencia y en la fase 1 se recabará la información completa sobre dicho tratamiento. En este mismo momento, se deberá entregar dicha información al DPD, con el objetivo de que éste pueda mantener actualizado el *Registro de Actividades de Tratamiento* de dicha institución. El DPD deberá ser una figura en la que los investigadores se podrán apoyar en todo momento para lograr una gestión adecuada de este tipo de procesos.

2. *Revisión del riesgo del proyecto*.

En la fase 2 de la metodología se plantea un modelo para que los investigadores puedan realizar un análisis básico de riesgos sobre cada uno de los tratamientos y, en segundo lugar, sobre el proyecto como tal, siempre desde el punto de vista de la gestión de los datos personales. Se trata de una herramienta de concienciación, útil para que el grupo conozca, desde un primer momento, el grado de complicación que puede llegar a tener un proceso de este tipo. En todos aquellos casos en los que surjan tratamientos clasificados como de alto riesgo o si el proyecto global es clasificado como de alto riesgo, será necesario contactar con el DPD de la institución responsable y comunicar este hecho. Es probable que, en estos casos,

sea necesario llevar a cabo una *Evaluación de Impacto en Protección de Datos* (EIPD). Este proceso deberá ser coordinado directamente por el DPD y los responsables del proyecto de investigación deberán colaborar en todo lo que sean requeridos. Como referencia, la AEPD ha publicado una lista en la que se relacionan todos los supuestos en los que es obligatorio, por defecto, realizar una EIPD[10].

3. *Entrega de información al interesado y garantía del ejercicio de derechos.*

En las fases 3 y 4, se revisan los modos de informar a los interesados sobre el proyecto de investigación y los tratamientos de datos asociados. Los responsables del grupo de investigación deberán contactar con el equipo de comunicación de la institución responsable para poder articular el modo de publicación de dicha información. La opción más adecuada en este caso es la construcción de una web informativa sobre el proyecto sobre la que, además, se podrán publicar todos los formularios de gestión de los derechos por parte de los interesados.

4. *Aplicación de medidas de seguridad.*

Dependiendo de los tratamientos identificados y de los niveles de riesgo asociados, se deberán adoptar ciertas medidas de seguridad (técnicas y/o organizativas). Para ello, también será necesario contar con la ayuda del DPD de la institución responsable y quizá con los responsables de seguridad de la misma. Se deberán valorar todas las opciones disponibles, incluidas las posibilidades de anonimización y seudonimización.

5. *Programa de cumplimiento de protección de datos.*

Con toda la información localizada en el presente apartado, el DPD de la institución responsable podrá elaborar el correspondiente *Programa de Cumplimiento*, específico para los tratamientos de datos personales identificados. Este programa es un modelo de organización y gestión que deberá recoger los principios generales de actuación en la entidad, medidas de seguridad, procedimientos implantados (o por implantar), responsables, roles, y actividades de control. Esta medida será muy importante para que la institución responsable pueda acreditar el *Principio de responsabilidad proactiva* en la gestión de datos personales.

[10] Disponible en https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

5. Evaluación de la metodología.

El proceso de evaluación de la metodología sirve para determinar si ésta es efectiva para solucionar el problema planteado.

Como se ha indicado, el alcance de este trabajo ha sido el de plantear una metodología teórica para estandarizar las tareas administrativas y de gestión relacionadas con los datos de carácter personal incluidos en los proyectos de investigación universitaria. Dicho objetivo se ha alcanzado, pero la puesta en marcha efectiva (y práctica) de esta metodología requiere un despliegue que no está contemplado en este trabajo y que supondría, al menos, las siguientes tareas:

- Conversión de la memoria en un documento de instrucciones simplificado. Se descartarían los apartados sólo relacionados con la estructura académica de la memoria y se potenciarían los que describen los conceptos y la propia metodología, adoptando un lenguaje más adecuado para el entorno investigador y relajando ciertas expresiones legales.
- Adaptación y automatización de las plantillas reflejadas en los anexos. Se implantarían en sistemas de formularios inteligentes, con opciones lo más cerradas posible (implementadas, por ejemplo, con desplegables y con algoritmos de decisión), para guiar eficazmente a los investigadores en su cumplimentación.

Por otro lado, en la propuesta inicial de este *Trabajo Fin de Master*, se proponía el siguiente método de evaluación de la metodología:

> El modo de comprobar esta adecuación es proporcionar el modelo generado a varios grupos de investigación con proyectos activos, pedir que lo apliquen como si fueran a gestionar de nuevo el proyecto (sólo la parte de protección de datos de carácter personal) y analizar los resultados obtenidos. Comparando la gestión inicial y la documentación generada aplicando la propuesta, se podría valorar:
> - La posible mejora en la adecuación a RGPD y LOPDGDD.
> - La posible mejora en la gestión para el investigador.
> - La posible mejora en la obtención de información relevante para el responsable de los datos (la universidad).

Este método de validación basado en la aplicación y prueba completas de la metodología, aunque viable desde el punto de vista funcional, no es posible desde un punto de vista temporal. Un despliegue de la metodología sobre un número suficiente de proyectos de investigación reales supondría mucho tiempo de ejecución, tanto por parte de los investigadores (a los que, previamente, se debería formar adecuadamente) como por parte del autor en las tareas de asesoría individualizada sobre la implementación (y también de otros actores, como los DPD de las instituciones afectadas). Dado que el proceso tiene que

encajar dentro de los límites temporales impuestos por el calendario académico del máster en el que se incluye, obtener resultados aceptables en los plazos establecidos sería extremadamente complicado.

Por este motivo, se propone una alternativa de validación para la metodología basada en dos elementos:

1. Entrega de la memoria a un conjunto de investigadores universitarios para obtener su opinión anónima sobre la utilidad de la misma. Las opiniones sobre las potenciales ventajas que puede suponer la aplicación de la metodología se recogerán mediante el formulario suministrado en el *Anexo 6* de esta memoria. Se trata de evaluar la comprensión de la metodología y la percepción de mejora, al menos desde el punto de vista teórico.
2. Entrega de la memoria para su análisis y valoración a expertos. En este caso, se tantea la opinión de un experto en la gestión de tratamientos de protección de datos personales y también de un investigador con amplia trayectoria, experto también en la gestión y organización del proceso investigador. Se trata de evaluar si la metodología se ajusta a lo requerido organizativa y legalmente en ambos tipos de gestión.

Los resultados del proceso se detallan en los siguientes apartados.

5.1. Valoración de los investigadores universitarios.

Para realizar esta fase de la valoración se ha pedido la colaboración de 27 miembros de la comunidad universitaria de Universidad Europea Miguel de Cervantes, todos ellos investigadores o con alguna misión relacionada directamente con la investigación universitaria. Debido a la estrechez de los plazos, únicamente se ha podido incluir en esta memoria la respuesta anónima de 20 de ellos.

Las características del conjunto de encuestados cuya opinión se incluye son las siguientes:

- 13 son doctores activos en investigación.
- 4 son doctorandos.
- 3 no son doctores, pero participan en distintos proyectos de investigación o en tareas de gestión directamente relacionadas con la investigación.
- Las áreas de conocimiento a las que pertenecen son: ciencias de la salud (60%), ciencias sociales (15%), ciencias naturales (10%), ciencias biomédicas (5%), ciencias experimentales (5%) y enseñanzas técnicas (5%).
- Todos los encuestados han participado, en mayor o menor medida, en proyectos de investigación (o lo están haciendo en este momento).

- El 80% de los encuestados afirma haber participado o estar participando en proyectos que incluyen trabajo con datos personales.

Tras pedir una lectura completa de la memoria, en el cuestionario se trata de recoger las siguientes medidas de opinión (globales y sobre algunos elementos concretos):

- Nivel de documentación aportada para aclarar los conceptos incluidos en la metodología.
- Nivel de comprensión de la metodología por parte del encuestado.
- Percepción de la complejidad de uso de la metodología.
- Percepción de mejoras para el investigador ante una posible aplicación práctica de la metodología en la gestión de proyectos con datos personales.

Resultados.

Para interpretar los resultados, se ha elegido la media aritmética (función *PROMEDIO* - Microsoft Excel) para medir la centralización o centro de gravedad de la distribución estadística y la desviación típica o estándar de la muestra (función *DESVEST.M* - Microsoft Excel) para medir la dispersión de los resultados.

Seguidamente, se recoge el promedio de las puntuaciones expresadas por los encuestados (junto con su desviación estándar muestral) sobre los conceptos recogidos en el cuestionario suministrado en el *Anexo 5*. Las puntuaciones expresadas se sitúan en un rango de 0 a 9, siendo 0 la puntuación más baja y 9 la más alta.

Valoración global de la metodología.

- (01) Grado de documentación de la metodología: 8,1 (σ=1,6)
- (02) Grado de comprensión general: 7,2 (σ=1,5)
- (03) Grado de complejidad de uso: 5,5 (σ=2,3)
- (04) Grado de posible mejora para el investigador en la gestión de proyectos con datos personales: 7,3 (σ=2,2)

Valoración sobre los procesos descritos en las distintas fases.

- Fase 0. Verificación de la existencia de tratamientos de datos personales e identificación de la fuente de los mismos.
  - (05) Grado de documentación de la fase: 8,3 (σ=1,2)
  - (06) Grado de comprensión general: 7,9 (σ=1,0)
  - (07) Grado de complejidad de uso: 4,4 (σ=2,5)
- Fase 1. Identificación de los tratamientos.
  - (08) Grado de documentación de la fase: 8,2 (σ=1,5)
  - (09) Grado de comprensión general: 7,5 (σ=1,4)
  - (10) Grado de complejidad de uso: 4,2 (σ=2,5)

- Fase 2. Identificación de riesgos y clasificación del proyecto.
  - (11) Grado de documentación de la fase: 8,2 (σ=1,8)
  - (12) Grado de comprensión general: 7,5 (σ=1,8)
  - (13) Grado de complejidad de uso: 4,9 (σ=2,6)

- Fase 3. Revisión del sistema de información al interesado, obtención del consentimiento y clausulado en formularios.
  - (14) Grado de documentación de la fase: 8,3 (σ=1,5)
  - (15) Grado de comprensión general: 7,7 (σ=1,6)
  - (16) Grado de complejidad de uso: 4,5 (σ=2,1)

- Fase 4. Implementación del ejercicio de derechos por parte de los interesados.
  - (17) Grado de documentación de la fase: 8,3 (σ=1,6)
  - (18) Grado de comprensión general: 7,7 (σ=1,3)
  - (19) Grado de complejidad de uso: 5,1 (σ=2,0)

- Fase 5. Aplicación de medidas de seguridad (investigadores y universidad).
  - (20) Grado de documentación de la fase: 8,1 (σ=1,8)
  - (21) Grado de comprensión general: 7,4 (σ=2,4)
  - (22) Grado de complejidad de uso: 5,8 (σ=2,2)

- Fase 6. Aplicación de anonimización y seudonimización.
  - (23) Grado de documentación de la fase: 8,2 (σ=1,5)
  - (24) Grado de comprensión general: 7,5 (σ=2,1)
  - (25) Grado de complejidad de uso: 4,9 (σ=2,9)

- Fase 7. Análisis de las implicaciones de los tratamientos.
  - (26) Grado de documentación de la fase: 8,3 (σ=1,3)
  - (27) Grado de comprensión general: 7,7 (σ=1,2)
  - (28) Grado de complejidad de uso: 4,5 (σ=2,5)

Valoración sobre las plantillas proporcionadas por la metodología.

- Plantilla Identificación de tratamiento de datos personales (*Anexo 1*).
  - (29) Grado de documentación de la plantilla: 8,1 (σ=1,7)
  - (30) Grado de comprensión general: 7,7 (σ=1,4)
  - (31) Grado de complejidad de uso: 4,2 (σ=2,6)

- Plantilla Identificación de riesgos en los tratamientos de datos personales (*Anexo 2*).
  - (32) Grado de documentación de la plantilla: 8,1 (σ=1,9)
  - (33) Grado de comprensión general: 6,8 (σ=2,2)
  - (34) Grado de complejidad de uso: 4,2 (σ=2,6)

- Plantilla Documento estándar de Consentimiento Informado (*Anexo 3*).
  - (35) Grado de documentación de la plantilla: 8,2 (σ=1,3)
  - (36) Grado de comprensión general: 7,9 (σ=1,0)
  - (37) Grado de complejidad de uso: 4,5 (σ=2,5)

- Catálogo general de amenazas y posibles soluciones, aplicable a los tratamientos de datos personales (*Anexo 4*).
  - (38) Grado de documentación de la plantilla: 8,1 (σ=1,5)
  - (39) Grado de comprensión general: 7,8 (σ=1,2)
  - (40) Grado de complejidad de uso: 4,3 (σ=2,6)

Un resumen de las principales sugerencias de mejora recogidas en los formularios es el siguiente:

- Necesidad de ejecutar acciones formativas concretas para investigadores.
- Utilizar un lenguaje más sencillo, sobre todo en los formularios a entregar a los interesados (*Anexo 3*).
- Aumentar la automatización de procesos lo más posible. Incluir herramientas como algoritmos de decisión, *check-list*s, formularios con desplegables cerrados, etc.
- Incorporar ejemplos que ilustren el uso de la metodología, incluyendo ejemplos prácticos de procesos de anonimización y seudonimización.
- Valorar la posible integración del consentimiento del tratamiento de datos con la aceptación voluntaria de participación en el estudio y/o proyecto.
- Describir los conceptos más claramente para facilitar las tareas a los no expertos en protección de datos.
- Ampliar información sobre anonimización y seudonimización. Profundizar en los posibles casos de identificación indirecta.
- Incluir desde las primeras fases de la metodología una participación activa obligatoria de los DPD de las instituciones afectadas.
- Simplificar lo más posible el proceso para no 'burocratizarlo' demasiado.

Valoración de los resultados.

Una vez más, reiterar que una validación completa y bien fundamentada de la metodología no se podrá llevar a cabo hasta que no se implemente completamente e incluya un modelo práctico y simplificado de aplicación. Pero, teniendo en cuenta esta consideración y, de los resultados obtenidos en la encuesta, se pueden extraer las siguientes conclusiones:

- De los resultados identificados en los ítems de puntuación global (1, 2, 3 y 4), y basado en las puntuaciones promedio, se puede extraer que:
    - La metodología está suficientemente documentada, de forma global, para los encuestados.
    - La muestra de encuestados ha comprendido, de forma general, la metodología.
    - El grado de complejidad de uso de la metodología es algo más elevado de lo previsto. Este parámetro deberá ser reducido con formación específica y en la fase de implementación práctica de la metodología.
    - Los investigadores encuestados piensan, con un promedio de 7,3, que la metodología puede ser útil en la gestión de proyectos con datos personales (aunque el índice de dispersión es ligeramente alto). Este es uno de los

parámetros que sugiere que, al menos para los encuestados, la metodología podría ser válida.

- En cuanto a la puntuación sobre las distintas fases (ítems 5 a 28), destaca:
    - El promedio del grado de documentación se mantiene en valores ligeramente superiores a 8.
    - En cuanto a la comprensión, los valores son superiores al 7,5.
    - Por lo que respecta a la complejidad de uso, las fases destacadas como más complejas serían la 5 (aplicación de medidas de seguridad) y la 4 (implementación del ejercicio de derechos por parte de los interesados). Efectivamente, se trata de fases cuya puesta en marcha puede ser compleja y deberá contar con la aportación de recursos importantes por parte de la universidad o universidades responsables del proyecto.
- Por lo que respecta a las plantillas (ítems 29 a 40), indicar que:
    - El promedio del grado de documentación es similar al del resto de elementos de la memoria.
    - Por lo que respecta a la comprensión, se desprende que será necesario trabajar, mediante las acciones de formación necesarias, en explicar los objetivos y el funcionamiento de la plantilla de identificación de riesgos en los tratamientos.
    - En cuanto a la complejidad de uso, no existen elementos que destaquen especialmente.

Importante añadir que, durante la fase de contacto con los encuestados, entrega del cuestionario y resolución de dudas con respecto a la lectura de la memoria y cumplimentación de la encuesta, el autor de este estudio ha podido percibir los siguientes problemas:

- La necesidad fundamental (ya identificada como requisito para la aplicación de la metodología en esta memoria) de establecer procesos formativos específicos sobre protección de datos de carácter personal para el colectivo de investigadores.
- En algunos casos se confunde lo que es un tratamiento de datos personales identificados (con aplicación de RGPD o LOPDGDD) y lo que es un tratamiento de datos con alguna característica asociada a personas, pero en el que no hay identificación (y, por tanto, al que no se le aplica RGPD o LOPDGDD).
- Existen notables diferencias entre las sensibilidades frente a los tratamientos de datos personales entre unos investigadores y otros. Probablemente, sean debidas a la experiencia y a la formación recibida al respecto.

5.2. Valoración de expertos.

Valoración 1. Experto en gestión de protección de tratamientos de datos personales.

Rodrigo Martín García, director de proyectos y responsable del área de Seguridad de la Información en *Symbiosis Consultores*, con más de 12 años de experiencia en proyectos de implantación, auditoría y revisión protección de datos basados tanto en la ya derogada LOPD como en las actuales legislaciones vigentes RGPD y LOPDGDD. Durante este periodo de tiempo, ha desarrollado diferentes proyectos con todo tipo de organizaciones públicas y privadas incluyéndose proyectos relacionados con la protección de datos en investigación.

Además, es especialista en la implantación y auditoría de *Sistemas de Gestión de Seguridad de la Información* (SGSI) basados en la Norma ISO/IEC 27001:2013 habiendo participado en diferentes proyectos de implantación y de mejoras de procesos de seguridad basados en esta Norma.

- *Identificación de tratamientos.*

La metodología planteada está compuesta por diferentes fases bien diferenciadas en las que se parte de una identificación del tratamiento de datos de carácter personal en la investigación universitaria por parte del investigador y, a su vez, la fuente de los datos recibidos (Fase 0). Unido a este primer paso, este deberá llevar a cabo el estudio del tipo de tratamientos de datos de carácter personal, así como de la licitud de tratamiento de los mismos y, llegado el caso, la comunicación al DPD como persona especialista de apoyo en la organización (Fase 1). Ambas fases, son fundamentales con el fin de poder abordar el proyecto de investigación con las garantías adecuadas y teniendo siempre en cuenta la aplicación de la privacidad desde el diseño y por defecto.

- *Actuación.*

Descrita entre las fases 2 y 6, ambas incluidas, supone el proceso a llevar a cabo una vez identificado adecuadamente el tratamiento de los datos de carácter personal en el proyecto de investigación con el fin de poder aplicar los procedimientos y medidas de seguridad adecuados en cada caso. Así, se parte de una identificación y clasificación del proyecto en base a los riesgos que permitirá, en los casos de riesgos de nivel medio y alto, la colaboración del DPD y la coordinación de las principales medidas a llevar a cabo tanto a nivel técnico como organizativo teniéndose en cuenta la importancia de cumplir con la información al interesado, aplicar las medidas de seguridad necesarias en función del tipo de datos tratados, generar los procedimientos para el ejercicio de los derechos y,

si fuese posible, llevar a cabo medidas de seudonimización y anonimización dentro del proyecto de investigación.

- *Revisión y evaluación de los tratamientos.*

Como última fase de esta metodología (Fase 7), se plantea un proceso de evaluación por parte del DPD y la posterior implementación en el proyecto de investigación del resultado final de las medidas y protocolos en cada caso.

La metodología planteada es acertada de cara a que todos los investigadores dentro de una Universidad estén obligados a tener en cuenta el cumplimiento de la legislación en materia de protección de datos antes del inicio de sus proyectos, se evalúen los riesgos del desarrollo de ese proyecto y se establezcan unas garantías gracias al seguimiento de un proceso en el que se tienen en cuenta todos los hitos necesarios para el cumplimiento del RGPD.

- *Propuesta de mejora.*

Dado que el cumplimiento de la legislación en materia de protección de datos es algo no suficientemente conocido por la mayoría del personal investigador, sería importante, la formación del mismo en la materia para que esta metodología fuese realmente útil y bien aplicada.

Además, como parte de esta metodología, sería interesante establecer auditorías de revisión y cumplimiento periódicas para aquellos proyectos de investigación de larga duración en el tiempo y que se puedan considerar de mayor riesgo con el fin de verificar que se está cumpliendo con lo establecido como consecuencia de la aplicación de la metodología.

Valoración 2. Experto en gestión de investigación universitaria.

Alejandro Santos Lozano, PhD, investigador con más de 10 años de experiencia en el área de biomedicina y fisiología (ODCID: orcid.org/0000-0002-2309-3583). Experto en epidemiología y aspectos clínicos y beneficios de la actividad física (o 'ejercicio') sobre la salud, siendo autor de +100 artículos indexados en *Journal Citation Report* (JCR) e investigador principal y colaborador en múltiples investigaciones y ensayos clínicos con humanos. Pertenece al grupo de investigación *i+12* del Hospital 12 de Octubre de Madrid (Madrid) y al *i+HeALTH* de la de la Universidad Europea Miguel de Cervantes (Valladolid).

Durante los años 2015 a 2019 fue director del Departamento de Ciencias de la Salud en la Universidad Europea Miguel de Cervantes, donde actualmente es Vicerrector de Internacionalización, Cultura Científica y Transferencia.

- *Adecuación de la metodología al sistema de gestión de la investigación en el ámbito universitario.*

El presente trabajo desarrolla un modelo de aplicación en RGPD y LOPDGDD en proyectos de investigación universitaria basado en 7 fases y resumido visualmente en la figura 2. En los últimos años a nivel mundial, debido fundamentalmente al incremento en el número de dispositivos móviles y a la mejora de sus tecnologías para registrar y compartir información de carácter personal y clínico, se ha profundizado en el desarrollo de legislaciones de protección de datos de esta naturaleza. Así, en nuestro país, muchos investigadores se encuentran en un estado de formación para adecuar sus metodologías de trabajo, en muchos casos desactualizadas, a la legislación actual.

Un modelo centrado en un algoritmo de decisión en función de las características de las investigaciones, como el que aquí se propone, puede ayudar a los investigadores y a los gestores de investigación de las universidades o institutos de investigación a actuar acorde con la normativa vigente. Por tanto, la metodología aquí propuesta puede ser de gran utilidad.

- *Opinión personal sobre la posible validez de la misma.*

La estructura de nuestro país, debido a la descentralización administrativa, confiere peculiaridades que en muchos casos complican el desarrollo de las investigaciones científicas cuando existen datos clínicos en la misma. A este respecto, y dado que cada comunidad autónoma tiene competencias propias, cada una de ellas puede tener características que confieren factores de confusión a los investigadores a la hora de tratar y manejar los datos anteriormente mencionados. Esta realidad, junto con la necesidad de cumplir con la Normativa Nacional y el Reglamento Europeo, hará que una metodología como la expuesta en esta memoria ayude a los investigadores en el diseño de sus investigaciones cumpliendo la normativa vigente, y será imprescindible para ellos, así como para la institución en la que desarrollan su actividad.

- *Aspectos a mejorar.*

Tal y como indica el autor de la propuesta en sus conclusiones, la metodología debería estar acompañada de un entorno que facilitara la ejecución práctica de la misma. La implementación del algoritmo en una aplicación desarrollada en entornos compatibles con dispositivos móviles (Windows, OSx. Android o iOS) con una interfaz de usuario amigable, mejoraría sustancialmente la propuesta. Así mismo, sería interesante que el autor actualizará la aplicación para mantenerla al día, ya que probablemente la legislación en el área seguirá sufriendo modificaciones.

6. Conclusiones y líneas futuras.

La garantía y gestión del derecho fundamental a la protección de los datos de carácter personal ha evolucionado y todos los procesos que se basen en el tratamiento de este tipo de datos se deben adaptar a esta evolución.

En el caso abordado en esta memoria, el problema principal detectado consiste en la falta de protocolos o procedimientos que ayuden a gestionar, regular y proporcionar seguridad al trabajo con datos personales en aquellos proyectos de investigación universitaria que los utilizan.

Con esta contribución, se ha realizado un estudio de las diferentes normativas intervinientes en los campos, por un lado, de la gestión de la protección de datos de carácter personal y, por otro, de la investigación universitaria (sobre todo, en aquellos casos en los que los procesos de investigación involucran el estudio de datos personales –sensibles o no-). Se ha tratado de lograr una integración de los mismos y el resultado se ha plasmado en una metodología que intenta agilizar y facilitar la gestión a los investigadores universitarios y también lograr que los tratamientos derivados sean lo más seguros posible, de forma que se puedan salvaguardar en todo momento los intereses de los afectados. Además, se ha tenido en cuenta la nueva normativa publicada, tanto en la Unión Europea (el RGPD) como en España (la LOPDGDD).

Si bien es cierto que la metodología propuesta aún debe ser completada con un entorno de ejecución práctico, contempla todos aquellos aspectos que deben ser tenidos en cuenta para que los tratamientos de datos personales incluidos en los proyectos de investigación se adecúen a los requisitos de la nueva normativa publicada, incorpora las suficientes garantías de seguridad para que los derechos de los afectados sean correctamente atendidos, e incluye herramientas que permitirán a los gestores de los proyectos de investigación ser más ágiles en la gestión de este apartado de sus proyectos.

Es fundamental resaltar que, para que ésta metodología sea efectiva, deberá llevarse a cabo un proceso previo de formación y concienciación a los usuarios de la misma (investigadores) sobre la utilización de los datos de carácter personal. Por muy alto que sea el nivel de automatización que se logre en la gestión de este tipo de proyectos, los resultados pueden no ser los adecuados si los investigadores no han asumido correctamente los conceptos manejados en el área de la protección de datos.

En cuanto a las líneas futuras de trabajo, se pueden identificar varios tipos de actuaciones:

- Conversión de esta memoria en un documento de instrucciones entregable a los investigadores. Dicha conversión debe generar un documento con una redacción más simple que emplee un lenguaje coloquial. Deberá adaptar los apartados iniciales de la memoria a la creación de un modelo teórico comprensible por lectores no habituados a textos jurídicos y deberá expresar las fases de la metodología en un modelo más cómodo de manejar, incorporando la ayuda de infografías, esquemas gráficos, etc. También será muy importante incluir ejemplos de utilización de distintos tipos de tratamiento.
- Automatización de las plantillas. Los modelos presentados en los Anexos 1, 2 y 3 pueden ser incluidos en un proceso de automatización, basados en diagramas de flujo y/o algoritmos de decisión. La mejor forma de hacerlo sería diseñar una web conectada a una base de datos que acumule la información de los sucesivos proyectos. Algunas de las tareas a automatizar serían:
    - En la plantilla de Identificación de tratamientos de datos personales, se podría dar de alta cada uno de los tratamientos. En los distintos campos a cumplimentar, se podrían sugerir contenidos mediante tablas desplegables u otras opciones similares. Esto facilitaría mucho el trabajo a los investigadores, pues tendrían las referencias concretas en cada caso y cumplimentar estos formularios sería mucho más sencillo.
    - Una vez cumplimentada la plantilla de Identificación de Tratamientos, habrá muchos campos que puedan servir para conectar con las plantillas de Identificación de Riesgos y, sobre todo, para el Consentimiento Informado. La automatización en este último caso, sería bastante alta.
- Diseño de plantillas para una web informativa de proyecto de investigación y formularios de gestión de derechos, que pudiera estar conectada a la misma base de datos y, por tanto, a la información obtenida de las plantillas automatizadas descritas en el punto anterior.
- Proceso de refinamiento y ajuste de las plantillas *Identificación de tratamiento de datos personales* e *Identificación de riesgos en los tratamientos de datos personales*, basado en los datos acumulados en las sucesivas aplicaciones de la metodología.
- Proceso de consulta sobre los tipos de proyectos de investigación realizados en las universidades españolas y, en concreto, sobre los que incorporan datos personales. El objetivo sería tratar de localizar los datos que más se utilizan para así ajustar los modelos lo mejor posible.

- Ampliación y ajuste de las amenazas y medidas o soluciones recogidas en el catálogo del *Anexo 4*, para adaptarlas lo más posible a los casos que se pueden encontrar en el ámbito de la investigación universitaria. Este proceso también se debe basar en los datos acumulados en las sucesivas aplicaciones de la metodología.

Referencias bibliográficas.

Agencia Española de Protección de Datos. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. Recuperado de https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

Agencia Española de Protección de Datos. (2017). *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*. Recuperado de https://www.aepd.es/media/guias/guia-directrices-contratos.pdf

Agencia Española de Protección de Datos. (2017). *Guía para el cumplimiento del deber de informar*. Recuperado de https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

Agencia Española de Protección de Datos. (2018). *Esquema de certificación de Delegados de Protección de datos de la AEPD (esquema AEPD-DPD)*. Recuperado de https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf

Agencia Española de Protección de Datos. (2018). *Guía práctica de Análisis de Riesgos en los tratamientos de datos personales sujetos al RGPD*. Recuperado de https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

Agencia Española de Protección de Datos. (2018). *Guía práctica para las Evaluaciones de Impacto en la protección de los datos sujetas al RGPD*. Recuperado de https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

Agencia Española de Protección de Datos. (2018). *Protección de Datos: Guía para el Ciudadano*. Recuperado de https://www.aepd.es/media/guias/guia-ciudadano.pdf

Agencia Estatal de Investigación. (s. f.). *Estructura de áreas y paneles científico técnicos*. Recuperado de http://www.idi.mineco.gob.es/portal/site/MICINN/menuitem.8ce192e94ba842bea3bc811001432ea0/?vgnextoid=fa347440163e5310VgnVCM1000001d04140aRCRD&vgnextfmt=default

Asociación Médica Mundial. (1964). *Declaración de Helsinki de la AMM – Principios éticos para las investigaciones médicas en seres humanos*. Recuperado de https://www.wma.net/es/policies-post/declaracion-de-helsinki-de-la-amm-principios-eticos-para-las-investigaciones-medicas-en-seres-humanos/

Constitución Española. (1978). *Boletín Oficial del Estado, núm. 311, de 29 de diciembre de 1978, páginas 29313 a 29424*. Recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. (1981). *Consejo de Europa*. Recuperado de https://www.boe.es/boe/dias/1985/11/15/pdfs/A36000-36004.pdf

Convention for the protection of individuals with regard to the processig of personal data. Convention 108+. (2018). *Consejo de Europa*. Recuperado de https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

CRUE Universidades Españolas. (2019). *Guía de buenas prácticas en materia de Transparencia y Protección de Datos*. Recuperado de http://www.crue.org/Documentos%20compartidos/Publicaciones/Gu%C3%ADa%20de%20buenas%20pr%C3%A1cticas%20en%20materia%20de%20Transparencia%20y%20Protecci%C3%B3n%20de%20Datos/Gui%CC%81a%20de%20buenas%20pra%CC%81cticas_VD.pdf

Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales. (1980). *Organización para la Cooperación y Desarrollo Económicos*. Recuperado de http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

España. Ley 14/2007, de 3 de julio, de Investigación Biomédica. *Boletín Oficial del Estado, núm. 159, de 4 de julio de 2007, páginas 28826 a 28848*. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2007-12945

España. Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. *Boletín Oficial del Estado, núm. 131, de 2 de junio de 2011*. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2011-9617

España. Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. *Boletín Oficial del Estado, núm. 155, de 29 de junio de 1985*. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-1985-12534

España. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. *Boletín Oficial del Estado, núm. 274, de 15 de noviembre de 2002*. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188

España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado, núm. 294, de 6 de diciembre de 2018, páginas 119788 a 119857*. Recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16673

España. Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades. *Boletín Oficial del Estado, núm. 89, de 13 de abril de 2007, páginas 16241 a 16260*. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2007-7786

España. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. *Boletín Oficial del Estado, núm. 262, de 31 de octubre de 1992, páginas 37037 a 37045*. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

España. Ley Orgánica 6/2001, de 21 de diciembre, de Universidades. *Boletín Oficial del Estado, núm. 307, de 24 de diciembre de 2001*. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2001-24515

España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado, núm. 298, de 14 de diciembre de 1999, páginas*

43088 a 43099. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

España. Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos. *Boletín Oficial del Estado, núm. 307, de 24 de diciembre de 2015, páginas 121923 a 121964*. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2015-14082

European Commission. (2019). *Horizon 2020 Programme Guidance. How to complete your ethics self-assessment*. Recuperado de https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

Grupo de Trabajo del Artículo 29 sobre Protección de Datos. (2018). *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*. Recuperado de https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Posas, F. (2018). La investigación y su papel en el futuro de la Universidad. *Revista de la Sociedad Española de Bioquímica y Biología Molecular*, *196*. Recuperado de https://www.sebbm.es/revista/articulo.php?id=475&url=la-investigacion-y-su-papel-en-el-futuro-de-la-universidad

Real Academia Española. (2014). *Diccionario de la lengua española (23ª edición)*. Recuperado de https://dle.rae.es/?id=M3a7YOZ

Unión Europea. Convenio para la protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. *Boletín Oficial del Estado, núm. 243, de 10 de octubre de 1979, págs. 23564 a 23570*. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010

Unión Europea. 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). *Diario Oficial de las Comunidades Europeas, núm. 119, de 4 de mayo de 2016, páginas 1 a 88*. Recuperado de https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa

Versión consolidada del Tratado de Funcionamiento de la Unión Europea. (2010). *Diario Oficial de la Unión Europea*. Recuperado de https://eur-lex.europa.eu/resource.html?uri=cellar:2563a53a-9617-4f41-9268-7d21b62926c1.0008.01/DOC_1&format=PDF

Anexo 1. Plantilla Identificación de tratamiento de datos personales.

Formulario de recogida de información para el Registro de Actividades de Tratamiento de Datos de Carácter Personal.

Datos principales.

1. Proyecto de investigación.

   [Identificar el nombre del proyecto de investigación al que se asocia el tratamiento de datos personales y resumir las principales características y objetivos del mismo]

2. Miembros del grupo de investigación.

   [Datos personales y de contacto del investigador principal del proyecto y del resto de miembros intervinientes en el mismo]

3. Actividades del tratamiento.

   [Identificar y describir:
   - El conjunto de operaciones, procedimientos o procesos, ya sean automatizados o manuales, que conlleven la recogida, consulta, grabación, modificación, cesión, destrucción, etc. de datos de carácter personal en este tratamiento.
   - La utilidad del tratamiento dentro del proyecto.
   - El ciclo de vida de los datos, desde su captura hasta su destrucción, incluyendo las tecnologías utilizadas en los procesos y los roles de usuario implicados.]

4. Finalidades.

   [Identificar y describir las finalidades concretas para las que se recaba cada tipo de datos dentro de las actividades del tratamiento que se llevan a cabo. Ejemplos:
   - Se recaban datos de contacto para enviar al interesado comunicaciones sobre …
   - Se recaban datos del historial médico sobre determinada patología para realizar un estudio sobre…
   - Se recaban datos sobre fotografías del rostro para diseñar un logaritmo de reconocimiento facial.
   - Con las categorías de datos …. y ….., se realizarán procedimientos de perfilado automático en base a los criterios de …]

5. Entidades responsables del tratamiento.

   [Identificar todas las entidades u organismos que intervienen en el proyecto y que disponen de capacidad de decisión sobre la actividad del tratamiento (universidad o universidades, entidades promotoras del proyecto, etc.)]

6. Delegados de Protección de Datos.

   [Identificar los DPD de todas las entidades enumeradas en el punto anterior que dispongan de esta figura]

7. Legitimación del tratamiento (licitud).

[Marcar la casilla o casillas adecuadas (en proyectos de investigación, normalmente la licitud viene dada por la primera opción o por la última de reutilización)]

☐ Consentimiento informado expreso de los interesados.

☐ Tratamiento necesario para cumplir un contrato entre interesado y responsable.

☐ Tratamiento necesario para el cumplimento de una obligación legal del responsable.

☐ Tratamiento necesario para proteger intereses vitales del interesado u otra persona física.

☐ Tratamiento necesario para el cumplimiento de una misión realizada en interés público.

☐ Tratamiento necesario para satisfacer intereses legítimos perseguidos por el responsable o por un tercero, siempre que dichos intereses no prevalezcan sobre los derechos y libertades fundamentales de los interesados.

Supuestos especiales:

☐ Tratamiento llevado a cabo sin consentimiento por autoridades sanitarias e instituciones públicas en acción de investigación para la vigilancia de la salud pública en situaciones graves.

☐ Tratamiento que reutiliza datos personales para investigación en materia de salud, tras disponer de consentimiento inicial para otra finalidad en áreas científicas relacionadas.

8. Interesados.

[Identificar y describir las categorías, colectivos o grupos de personas físicas identificadas o identificables a quien corresponden los datos personales que son tratados.]

9. Categorías de datos personales.

[Proporcionar detalle de los datos objeto del tratamiento:

- Datos identificativos (nombre y apellidos; DNI, NIF, pasaporte o similar; Número de Seguridad Social, dirección postal; correo electrónico; teléfono; fax; dirección IP pública; imagen o voz; firma manuscrita; huella digital; certificado digital; etc.).
- Datos de características personales (estado civil, datos familiares, lugar y fecha de nacimiento, edad, lengua materna, características físicas y antropométricas, etc.).
- Datos multimedia (foto, vídeo o audio que recojan al interesado).
- Datos económico-financieros (cuenta bancaria, solvencia, datos sobre inversiones, créditos, nómina, ingresos, rentas, etc.).
- Datos de circunstancias sociales (propiedades, alojamiento, aficiones y estilos de vida, membresías a asociaciones o clubs, etc.).
- Datos de carácter social (prestaciones, ayudas, pensiones, etc.).
- Datos académicos y profesionales (formación, titulaciones, expediente académico, profesión, experiencia, currículum vitae, pertenencia a colegios profesionales, datos sobre el empleo, etc.).
- Datos sensibles o especialmente protegidos:
  - Datos sindicales.
  - Datos de salud o médicos (historial clínico, enfermedades, alergias, etc.).
  - Datos ideológicos, religiosos y políticos.

- Datos de origen racial o étnico.
- Datos relacionados con la orientación y vida sexual.
- Datos biométricos (ADN, huellas digitales, iris, patrones faciales, etc.).
- Datos administrativos o judiciales (procedimientos administrativos, recursos, expedientes, sanciones, condenas, registros, etc.).

- Otros tipos de datos personales (especificar).

  Es fundamental tener en cuenta que los datos recogidos deben ajustarse al principio de *Minimización de los datos*, es decir, ser adecuados, pertinentes y no excesivos (limitados a lo necesario), tomando como base las finalidades concretas del tratamiento dentro del proyecto.]

10. Cesiones de datos previstas (si las hubiera).

    [Describir las categorías de destinatarios a quienes se comunicarán los datos personales, incluyendo también los posibles destinatarios en otros países u organizaciones internacionales. Es importante diferenciar entre cesión de datos y el acceso a los mismos por parte de terceros autorizados (encargados de tratamiento). Especificar la base jurídica que soporta la cesión (consentimiento, obligación legal, etc.)]

11. Transferencias de datos internacionales previstas (si las hubiera).

    [Identificar las transferencias internacionales de los datos. Se debe indicar el país u organización internacional de destino, junto a la base jurídica que hace posible la transferencia.]

12. Período de conservación de los datos (mínimo-máximo).

    [Describir los plazos de conservación de la información (mínimos y máximos), establecidos dentro del ciclo de vida del tratamiento. Deberán tenerse en cuenta la función y las finalidades del tratamiento, así como la categoría del dato, el principio de *Limitación del plazo de conservación* y lo dictado por otras normativas aplicables.]

13. Medidas de seguridad adoptadas por las entidades responsables del tratamiento.

    [Describir, de modo general, las medidas técnicas (a nivel informático) y organizativas (procedimientos) de seguridad aplicables al entorno en que se llevarán a cabo las tareas asociadas al proyecto de investigación.]

Información sobre Encargados de tratamiento (si los hubiera).

1. Encargados del tratamiento.

   [Enumerar las personas físicas o jurídicas, autoridades públicas, servicios u otros organismos que puedan prestar el servicio de tratamiento identificado por cuenta de los responsables enumerados en el primer punto del formulario.]

2. Descripción de los tratamientos.

   [Describir, para cada caso, el objeto del tratamiento, la duración, finalidad, tipos de datos personales manejados y categorías de interesados.]

3. Transferencias de datos (si las hubiera).

   [Identificar y describir las posibles transferencias a terceros encargados de tratamiento, incluidas las internacionales.]

4. Medidas de seguridad adoptadas por los encargados (si las hubiera y se conocen).

   [Describir, de modo general, las medidas técnicas (a nivel informático) y organizativas (procedimientos) de seguridad aplicables al entorno en que se llevarán a cabo las tareas asociadas al proyecto de investigación por parte del encargado.]

Otros datos.

[Incorporar cualquier otra información considerada como oportuna en este proceso.]

Anexo 2. Plantilla Identificación de riesgos en los tratamientos de datos personales.

Formulario de Identificación de riesgos.

Posibles amenazas		Si / No	Riesgo
Tratamientos a gran escala[11].	Cuantificación sujetos afectados.		A
	Duración del ciclo de vida del tratamiento.		A
Observación y monitorización sistemáticas de aspectos personales.	Detección de patrones de hábitos, preferencias, intereses, etc.		A
Tipos de datos personales tratados.	Tratamiento de datos de más de 5 categorías especificadas en el punto 9 de la plantilla registrada en el Anexo 1 de esta memoria.		A
	Tratamiento de datos especialmente protegidos		A
Contacto con afectados considerado como intrusivo	Llamadas telefónicas		M
	Vigilancia electrónica, biometría, técnicas genéticas, minería de datos, geolocalización, etc.		A
Tratamiento que implica el uso de datos genéticos para cualquier fin.			A
Uso de datos de afectados con discapacidades, menores de 14 años o colectivos en situación de especial vulnerabilidad			A
Tratamiento para elaborar perfiles, categorizar o segmentar, hacer ratings o scoring.			M
Tratamiento que impliquen tomas de decisiones automatizadas (sin intervención de personas que decidan o valoren resultados)			A
Tratamiento que añada nuevas categorías de información personal a los datos ya existentes o que use los datos existentes para finalidades no contempladas en el consentimiento inicial.			A
Tratamiento que implique el acceso de un elevado número de personas a los datos (más allá de las necesarias para llevarlo a cabo)			M
Tratamiento relativo a la observación de zonas de acceso público (excluyendo lugares de trabajo).			M
Tratamiento de datos no anonimizados con fines estadísticos, históricos o de investigación científica.			M
Tratamiento de datos que utiliza tecnologías inmaduras o de reciente implantación.			A
Tratamiento en el que se producen cesiones de datos.			B
Transferencias internacionales de datos	Unión Europea		B
	Países declarados como “de nivel adecuado” por la Comisión Europea[12]		B
	Otros		M
Medidas de seguridad aplicadas en el tratamiento	Se conocen y se consideran adecuadas		B
	Se conocen y no se consideran adecuadas		M
	No se conocen		M
Percepción de existencia de riesgo por parte del investigador.	El tratamiento es similar a otro que ya ha sido considerado como de riesgo		M
	El tratamiento puede llegar a suponer una pérdida o alteración de la información personal		M
Tratamiento con documentación en papel	La documentación no se protege bajo llave		M
	No existe inventario actualizado de los datos		B
	No se mantiene un registro de accesos a la información		B
	La información no se destruye de forma segura		M

[11] Consultar la guía WP243 “Directrices sobre los delegados de protección de datos (DPD)” del *Grupo de Trabajo del Artículo 29* para determinar si el tratamiento es a gran escala. Disponible en https://www.aepd.es/media/criterios/wp243rev01-es.pdf

[12] Consultar información en la web de AEPD (https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales)

Posibles amenazas		Si / No	Riesgo
Intervención de encargados de tratamiento	No intervienen		B
	Intervienen y la relación con el responsable está garantizada mediante contrato con arreglo a RGPD		B
	Intervienen y la relación con el responsable no está garantizada mediante contrato con arreglo a RGPD.		M
Necesidad y proporcionalidad del tratamiento	No se cumple el principio de limitación de la finalidad.		M
	No se cumple el principio de minimización de datos.		M
	No se cumple el principio de limitación del plazo de conservación.		M
	Las tecnologías empleadas no cumplen los principios fundamentales de la privacidad.		A

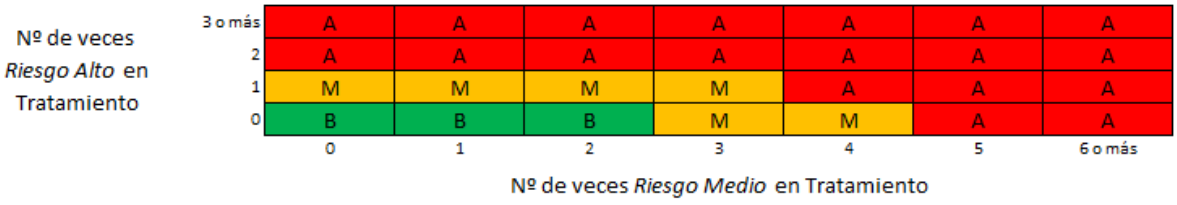
Niveles de riesgo para las distintas entradas:

- **A**: Alto.
- **M**: Medio.
- **B**: Bajo.

El investigador deberá indicar, para cada entrada de la tabla, si estima que las posibles amenazas especificadas pueden llegar a materializarse o no en el tratamiento.

La clasificación de riesgo del tratamiento se calcula mediante la contabilización de los niveles de riesgo individuales para todos aquellos casos en los que el investigador indica **SI** en la columna correspondiente (considerando sólo los niveles **Medio** y **Alto**). Los valores de riesgo resultantes para el tratamiento se obtienen ubicando el resultado de la anterior contabilización en el siguiente esquema:

Figura 5. Clasificación del tratamiento en base a los niveles de riesgo.



Fuente: elaboración propia.

Formulario basado en:

- Análisis de riesgos de la *Guía práctica de Análisis de Riesgos en los tratamientos de datos personales sujetos al RGPD* (Agencia Española de Protección de Datos, 2018).
- Diversos apartados de la *Guía práctica para las Evaluaciones de Impacto en la protección de los datos sujetas al RGPD* (Agencia Española de Protección de Datos, 2018).

Anexo 3. Plantilla Documento estándar de Consentimiento Informado.

Información básica relativa a la protección de sus datos personales.

Conforme a lo dispuesto en el 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 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), así como en la normativa específica vigente en cada momento, nos dirigimos a usted para invitarle a participar en un estudio de investigación universitario, promovido por *[organismo]* de la *[universidad]*.

Seguidamente, se proporciona información para que usted pueda decidir, de forma completamente voluntaria, si participa en el estudio.

Datos sobre el proyecto.

1. Nombre del estudio y pequeña descripción de los objetivos y actividades del proyecto de investigación en el que está enmarcado el tratamiento.

   [Nombre y descripción] [URL sobre información del mismo, si tuviera]

2. Responsable del tratamiento de datos personales.

   [Nombre responsable, normalmente la universidad]

3. Investigador responsable del proyecto.

   [Nombre IP]

4. Finalidad del tratamiento.

   [Mantener sólo la opción que mejor se adapte al tipo de proyecto. Si hubiera más finalidades, añadir]

   [Opción 1. Proyectos en los que los datos personales no son objeto de estudio] Las finalidades del tratamiento de datos personales son gestionar su participación en el [*proyecto de investigación*], así como remitirle comunicaciones en relación con el mismo a través de los siguientes medios: [*definir: correo electrónico, teléfono, etc.*].

   [Opción 2. Proyectos en los que los datos personales son objeto de estudio] Las finalidades del tratamiento de datos personales son gestionar su participación en el proyecto *[proyecto de investigación]* e incorporar sus datos personales de las categorías *[identificar categorías de datos que se utilizarán en el proyecto]* al mismo para su

estudio, publicar los resultados finales del estudio, así como remitirle comunicaciones en relación con el mismo a través de los siguientes medios: *[definir: correo electrónico, teléfono, etc.]*.

5. Anonimización y seudonimización.

   [Si el tratamiento incorporar alguno de estos procesos, indicarlo y describir su operativa. Sin no lo incluye, indicar 'No se llevan a cabo procesos de este tipo'.]

6. Plazos de conservación de los datos.

   [Si se conocen plazos concretos, indicarlos. Si no, dejar el siguiente párrafo genérico, adaptándolo a la situación concreta del proyecto.]

   Los datos serán conservados mientras sean necesarios para las finalidades de investigación científica que persigue el proyecto de investigación referenciado. Una vez finalizado el mismo, los datos podrán eliminarse de forma segura o anonimizarse para su conservación indefinida, debido al interés científico del estudio.

7. Legitimación.

   Consentimiento expreso del interesado, marcando las casillas dispuestas a tal efecto.

8. Destinatarios.

   Los datos personales no serán comunicados a terceros, salvo a posibles prestadores de servicios en el ámbito del proyecto, o por obligaciones legales.

9. Ejercicio de derechos.

   Puede ejercitar sus derechos de información, acceso, rectificación, supresión, oposición, limitación del tratamiento, oposición a decisiones individuales automatizadas y portabilidad mediante un escrito dirigido a *[dirección postal universidad responsable]*, o al correo electrónico *[correo electrónico DPD universidad responsable]*.

10. Procedencia de los datos (cuando no los proporciona directamente el interesado).

    [Indicar el tratamiento original del que proceden los datos y la legitimación para utilizarlos en el presente proyecto.]

Consulta de información ampliada en: *[URL de la política de privacidad publicada en la página web de la universidad responsable que recoja información avanzada sobre este tratamiento] [Otros contactos con los investigadores para obtener información.]*

Consentimientos.

Revisada la información sobre el proyecto de investigación referenciado, comprendo que mi participación en el estudio es voluntaria y que puedo retirarme del mismo en cualquier momento.

Doy libremente mi conformidad para que mis datos sean tratados por *[Nombre responsable, normalmente la universidad]*, con las finalidades siguientes: *[ajustarlas a las descritas en el punto 4]*

Si ☐ No ☐ Gestionar mi participación en el proyecto e incorporar mis datos personales (categorías identificadas en el punto 4) para su estudio.

Si ☐ No ☐ Incorporar mis datos personales (categorías identificadas en el punto 4), convenientemente anonimizados o seudonimizados[13] en la publicación de los resultados del estudio.

Si ☐ No ☐ Remitirme comunicaciones en relación con el proyecto.

Consentimientos especiales adicionales *[Utilizar sólo en caso necesario]*

Si ☐ No ☐ Consiento en que mis datos personales sean utilizados para elaborar perfiles automatizados en el ámbito de *[Describir]*.

Si ☐ No ☐ Consiento en que mis datos sean utilizados para la toma de decisiones automatizadas en el ámbito de *[Describir]*.

Consentimiento especial en relación con tratamientos de datos de salud.

En el proyecto de investigación mencionado se pueden llegar a tratar datos sobre su salud. Para poder utilizarlos con fines de investigación científica o docente, es necesario que otorgue su autorización a *[Nombre responsable, normalmente la universidad]*.

Don/doña, _____, con NIF _____, mayor de 14 años, consiente en el tratamiento de sus datos de salud en los términos indicados anteriormente.

Y para que así conste, firma la presente en _____, a __ de _____ de 20___.

Firmado: _____

Nota: en el caso de menores de 14 años o personas incapacitadas para prestar este consentimiento, deberá firmar el consentimiento el padre/madre o tutor legal.

[13] Nota. Los procesos de anonimización y seudonimización en el proceso de publicación de resultados del proyecto sirven para evitar que los datos personales publicados puedan asociarse directamente con la persona o personas a las que pertenecen, es decir, revelar su identidad.

Anexo 4. Catálogo general de amenazas y posibles soluciones, aplicable a los tratamientos de datos personales.

Catálogo extraído de los apartados *5.5 Anexo V: Catálogo de amenazas* y *5.6 Anexo VI: Catálogo de amenazas y posibles soluciones* de la *Guía práctica para las evaluaciones de impacto en la protección de datos personales* (Agencia Española de Protección de Datos, 2018) y adaptado para su aplicación en la gestión de proyectos de investigación que incorporen trabajo con datos personales:

1. Amenazas de tipo general.

Amenaza	Soluciones
1.1. Pérdidas económicas y daños reputacionales en las instituciones (incluidas universidades) derivados del incumplimiento de la legislación sobre protección de datos personales.	• Formación apropiada general para todo el personal de la institución sobre protección de datos • En caso de tratamientos asociados a proyectos de investigación universitarios, establecer procesos de formación específica sobre protección de datos orientada a gestión de proyectos de investigación a investigadores y PAS relacionados. • Comunicación auditable y clara de las responsabilidades del personal (PAS, PDI y PEI) en relación con el cumplimiento de las políticas de privacidad de la organización, así como de las sanciones aparejadas al incumplimiento de las mismas.
1.2. Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento.	• Formación específica sobre protección de datos orientada a gestión de proyectos de investigación a investigadores y PAS relacionados. • Comunicación auditable y clara de las responsabilidades del personal (PAS, PDI y PEI) en relación con el cumplimiento de las políticas de privacidad de la organización relativas a las legislaciones sectoriales que afectan a la organización, así como de las sanciones aparejadas al incumplimiento de las mismas.
1.3. Pérdidas económicas, pérdida de clientes (alumnos) y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales.	• Formación apropiada del personal (PAS, PDI y PEI) sobre seguridad y uso adecuado de las TIC. • En caso de tratamientos asociados a proyectos de investigación universitarios, proporcionar información a investigadores y PAS relacionados con los proyectos de investigación sobre medidas de

	seguridad concretas y usos adecuados de las TIC en los entornos utilizados en dichos proyectos de investigación. • Comunicación auditable y clara de las responsabilidades del personal (PAS, PEI y PDI) en relación con el cumplimiento de las políticas y las medidas de seguridad así como de las sanciones aparejadas al incumplimiento de las mismas.
1.4. Pérdida de competitividad del producto o servicio, o pérdida de validez en la acreditación de los resultados de los proyectos de investigación, derivadas de los daños reputacionales causados por una deficiente gestión de la privacidad.	• Formación apropiada del personal (PAS, PDI y PEI) sobre protección de datos, seguridad y uso adecuado de las TIC.
1.5. Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.	• Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella. • Nombrar un Delegado de Protección de Datos (que dependiendo del tamaño de la organización será una persona o un departamento interno o externo) para ocuparse de todas las cuestiones relativas a la privacidad dentro de la organización y contar con asesoramiento cualificado. Si se procede a este nombramiento, el Delegado de Protección de Datos puede hacerse cargo también de la interlocución con los afectados. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 4 de esta metodología para una correcta gestión del ejercicio de derechos por parte de los interesados.
1.6. Incorporación tardía de los expertos en protección de datos (en particular, del delegado de protección de datos o DPD) a los proyectos o definición deficiente de sus funciones y competencias.	• Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del DPD en las fases iniciales de los mismos. • Establecer desde la dirección las funciones, competencias y atribuciones del DPD en el desarrollo y gestión de los proyectos. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente la Fase 0 de esta metodología para implicar al DPD desde el comienzo de la gestión de los proyectos de investigación que trabajan con datos de carácter personal.

2. Legitimación de los tratamientos y cesiones de datos personales.

Amenaza	Soluciones
2.1. Tratar o ceder datos personales cuando no es necesario para la finalidad perseguida.	• Usar datos disociados o anonimizados siempre que sea posible y no implique un esfuerzo desproporcionado. • Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas. • Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas. • Evitar el uso de datos biométricos y/o genéticos salvo que resulte imprescindible o esté absolutamente justificado. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente las Fases 0 y 1 de esta metodología, consultando con el DPD para identificar correctamente los datos personales necesarios para el proyecto.
2.2. Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales.	• Formación adecuada del personal (PAS, PDI y PEI) sobre protección de datos, seguridad y uso adecuado de las TIC. • Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas. • Si es necesario, buscar asesoramiento experto. • Si se ceden datos personales, establecer por escrito acuerdos que contemplen las condiciones bajo las que se produce la cesión y, en su caso, las relativas a cesiones ulteriores, así como las posibilidades de supervisión y control del cumplimiento del acuerdo. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente la Fase 1 de esta metodología, para así tener identificadas correctamente la legitimación y las posibles cesiones de datos.
2.3. Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.	• Asegurarse de que no existen otras causas de legitimación más adecuadas.

	• Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato. • Evitar condicionar el disfrute de un producto o servicio al consentimiento para finalidades diferentes. • En el ámbito laboral, evitar basar los tratamientos de datos en el consentimiento de los trabajadores. • Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente la Fase 3 de esta metodología, para así disponer de un consentimiento adecuado.
2.4. Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión.	• Establecer procedimientos claros para manifestar la revocación del consentimiento o la solicitud de oposición a un determinado tratamiento. Si la organización realiza acciones publicitarias, tener en cuenta las reglas especiales existentes para las comunicaciones comerciales y, en particular, cuando estas se llevan a cabo a través de comunicaciones electrónicas. • Establecer los mecanismos necesarios para garantizar que se consultan los ficheros de exclusión de publicidad, tanto de la organización como externos, y que se tienen en cuenta los deseos de quienes se han inscrito en ellos. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 4 de esta metodología para una correcta gestión del ejercicio de derechos por parte de los interesados.
2.5. Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros.	• Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido legal y lealmente. • En la realización de campañas publicitarias con datos provenientes de terceros en las que se segmenta el público objetivo en función de parámetros determinados, exigir garantías de que

	las personas cuyos datos van a ser utilizados han dado su consentimiento para ello. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 0 de esta metodología para identificar correctamente la fuente de los datos y, en caso de tratamientos previos, verificar su si su consentimiento inicial es aplicable.
2.6. Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias.	• Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas. • Verificar si el tratamiento está amparado o es requerido por una ley. • En caso contrario, establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.
2.7. Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la reidentificación de información disociada.	• Verificar la legitimidad de la interconexión de datos prevista. • Definir claramente los datos personales resultantes del tratamiento y verificar tras el proceso que son los únicos que se han generado.
2.8. Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable.	• Verificar la legitimidad del tratamiento anónimo. • Implementar el acceso anónimo al tratamiento afectado.
2.9. Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada.	• Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies, etc.). • Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. • Respetar las preferencias establecidas por los afectados en sus navegadores sobre el rastreo de su navegación.

3. Transferencias internacionales.

Amenaza	Soluciones
3.1. Acceso secreto a los datos personales por parte de autoridades de terceros países.	• Incluir cláusulas de salvaguarda en las que se requiera información sobre el acceso a los datos

	personales transferidos por parte de autoridades de terceros países tan pronto como sea posible.
3.2. Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia.	• Si existen transferencias internacionales a países fuera del Espacio Económico Europeo, implantar los procedimientos de control necesarios (incluidos los contractuales) para garantizar que se cumplen las condiciones bajo las que se llevó a cabo la transferencia. En este sentido, hay que prestar especial atención cuando se contraten servicios de Cloud Computing u hospedados en terceros.
3.3. Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados.	• Asegurarse de la exigibilidad de mecanismos de control del importador tales como listas de encargados de tratamiento, países donde operan, posibilidad de revisar documentación y realizar auditorías, etc.
3.4. Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el importador.	• Asegurarse de la definición y funcionamiento de un canal de comunicación entre exportador e importador para hacer llegar las solicitudes y reclamaciones de los afectados. • Poner en marcha procedimientos que garanticen la adecuada atención de las demandas de los afectados. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 4 de esta metodología para una correcta gestión del ejercicio de derechos por parte de los interesados.
3.5. No obtención de las autorizaciones legales necesarias.	• Solicitar la autorización del Director de la Agencia Española de Protección de Datos en aquellos casos que resulte necesario.

4. Notificación y registro de las actividades de tratamiento.

Amenaza	Soluciones
4.1. Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe registrarse la creación, modificación o cancelación de actividades de tratamiento.	• Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente la Fase 1 de esta metodología, para así mantener actualizado el Registro de Actividades de Tratamiento (RAT).
4.2. Carecer de los mecanismos y procedimientos necesarios para detectar cuando debe realizarse análisis de impacto en protección de datos y su consulta a la autoridad de control.	• Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo.

	• En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente las Fases 1 y 2 de esta metodología, para así, por un lado, tener informado al DPD del tipo de datos personales tratados y de su finalidad; y, por otro, disponer de una medida inicial del riesgo del tratamiento.

5. Transparencia de los tratamientos.

Amenaza	Soluciones
5.1. Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (ubicación geográfica, comportamiento, hábitos de navegación, etc.).	• Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. • Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente la Fase 3 de esta metodología, para aportar la debida información a los interesados en el momento de la solicitud del consentimiento y la Fase 4, para asegurar que se proporciona correctamente el derecho de información a los interesados.
5.2. En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que dificulten su acceso conjunto y detallado.	• Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión. • Verificar que la información que se ofrece en todos los lugares y situaciones es coherente y sistemática. • Verificar que la información se ofrece en todos los formularios. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 3 de esta metodología, para aportar la debida información a los interesados en el momento de la solicitud del consentimiento y la Fase 4, para asegurar que se proporciona correctamente el derecho de información a los interesados..

5.3. Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales.	• Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización. • Analizar los perfiles de sujetos cuyos datos son analizados en los distintos proyectos de investigación universitarios con el objetivo de utilizar un lenguaje adaptado y de fácil comprensión para los mismos.

6. Calidad de los datos.

Amenaza	Soluciones
6.1. Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto, servicio o proyecto de investigación.	• Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente las Fases 0 y 1 de esta metodología, consultando con el DPD para identificar correctamente los datos personales necesarios para el proyecto.
6.2. Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas.	• Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la Organización que estén autorizados a utilizarlos. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 4 de esta metodología para una correcta gestión del ejercicio de derechos por parte de los interesados.
6.3. Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos.	• Siempre que sea posible, utilizar datos anónimos o disociados. • Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas. • Garantizar que se aplican las medidas de seguridad adecuadas y correspondientes al nivel de seguridad de los datos utilizados.

6.4. Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas: • Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas. • Toma de decisiones económicas, sociales, laborales, etc. relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables), especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes de servicios y productos o trabas para el paso de fronteras.	• Suministrar información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible. • Proporcionar información sobre los criterios utilizados en la toma de decisiones y permitir a los afectados impugnar la decisión y solicitar que sea revisada por una persona. • Proporcionar información sobre las medidas que se han implantado para lograr el necesario equilibrio entre el interés legítimo del responsable y los derechos fundamentales de los afectados. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente la Fase 3 de esta metodología, para así disponer de un sistema que aporte la debida información a los interesados.
• Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas. • Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas. 6.5. Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo.	• Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer. • Establecer posibilidades de impugnación ágiles para ofrecer vías de recurso adecuadas a los afectados. • Establecer canales alternativos para tratar con los falsos negativos y falsos positivos en la identificación y autenticación de personas a través de datos biométricos.
6.6. Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron.	• Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información. • Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de cancelación de la información. • Implantar mecanismos para llevar a cabo y gestionar dicha cancelación en el momento adecuado incluyendo, si corresponde, el bloqueo temporal de los datos personales. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 4 de esta metodología para una correcta gestión del ejercicio de derechos por parte de los interesados.

7. Categorías especiales de datos.

Amenaza	Soluciones
7.1. Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando este sea la causa que legitima su tratamiento o cesión.	• Evitar el uso de datos especialmente protegidos salvo que resulte absolutamente necesario. • Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente la Fase 3 de esta metodología, para así disponer de un consentimiento adecuado.
7.2. Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos de categorías especiales.	• Nombrar un Delegado de Protección de Datos (DPD) para contar con asesoramiento cualificado. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar correctamente la Fase 1 de esta metodología, para así tener identificadas correctamente la legitimación y las posibles cesiones de datos.
7.3. Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales en procesos de investigación que solo prevén utilizar datos anónimos.	• Utilizar técnicas de disociación que garanticen el anonimato real de la información o, al menos, que el riesgo residual de re-identificación sea mínimo.

8. Deber de secreto.

Amenaza	Soluciones
8.1. Accesos no autorizados a datos personales.	• Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. • Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de confidencialidad de la organización. • Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento. • Notificar que se dará traslado a las autoridades competentes de las violaciones de confidencialidad que puedan entrañar responsabilidades penales.

	• Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales.
8.2. Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización.	• Formación adecuada de los empleados (PAS, PDI y PEI) sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. • Establecimiento de sanciones disuasorias para los empleados (PAS, PDI y PEI) que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas.

9. Tratamientos por encargo.

Amenaza	Soluciones
9.1. Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.	• Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos.
9.2. Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento.	• Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia. • Establecer contractualmente mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros.
9.3. Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.	• Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado de tratamiento. • Realizar auditorías periódicas al encargado de tratamiento para verificar que cumple las estipulaciones del contrato. • Definir acuerdos de nivel de servicio que garanticen el correcto cumplimiento de las instrucciones del responsable y la adopción de las medidas de seguridad adecuadas.
9.4. No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos de los interesados realizados ante los encargados de tratamiento.	• Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados.

	• Definir los procedimientos operativos para que esta comunicación se lleve a cabo de forma ágil y eficiente.
9.5. Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato.	• Incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. • Establecer medidas técnicas y organizativas que garanticen la portabilidad.

10. Derechos de los interesados.

Amenaza	Soluciones
10.1. Dificultar o imposibilitar el ejercicio de los derechos de los interesados.	• Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos. • Evitar sistemas de ejercicio de los derechos de los interesados que impliquen solicitar una remuneración. • Evitar establecer procedimientos poco transparentes, complejos y laboriosos. • Formar a todo personal para que conozca qué ha de hacer si recibe una petición de derecho de los interesados o ha de informar a los afectados sobre cómo ejercerla. • Definir qué personas o departamentos se ocuparán de gestionar los derechos de los interesados y formarlos adecuadamente. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 4 de esta metodología para una correcta gestión del ejercicio de derechos por parte de los interesados.
10.2. Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados.	• Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos de los interesados y que pueden suministrar la información adecuada a los afectados. • Formación de los empleados encargados de gestionar los ejercicios de derechos de los interesados. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 4 de esta metodología para una correcta gestión del ejercicio de derechos por parte de los interesados.

10.3. Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales.	• Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate. • Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos. • Formación de los empleados encargados de gestionar los ejercicios de derechos de los interesados. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar la Fase 4 de esta metodología para una correcta gestión del ejercicio de derechos por parte de los interesados.

11. Seguridad.

Amenaza	Soluciones
11.1. Inexistencia de responsable de seguridad o deficiente definición de sus funciones y competencias.	• Nombramiento de un responsable de seguridad y establecimiento por parte de la dirección de sus funciones, competencias y atribuciones en el desarrollo y gestión de los proyectos.
11.2. Carencia de medidas de seguridad o aplicación deficiente las mismas.	• Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del responsable de seguridad en las fases iniciales de los mismos. • En caso de tratamientos asociados a proyectos de investigación universitarios, implementar las Fases 1 y 2 de esta metodología para que el DPD disponga de la información necesaria sobre el proyecto y pueda trasladar al responsable de seguridad las medidas técnicas y organizativas necesarias para asegurar el tratamiento.
11.3. Inexistencia de política de seguridad.	• Solicitud al responsable de seguridad para la elaboración de la política de seguridad.
11.4. Deficiencias organizativas en la gestión del control de accesos.	• Políticas estrictas de acceso a la información por necesidad de conocer (need to know) para la concesión de accesos a la información y de escritorios limpios de documentación (cleandesks) para minimizar las posibilidades de acceso no autorizado a los datos personales. • Establecer procedimientos que garanticen la revocación de permisos para acceder a datos

	personales cuando ya no sean necesarios (abandono de la organización, traslado, cambio de funciones, etc.). • Inventariar los recursos que contengan datos personales accesibles a través de redes de telecomunicaciones. • Inventariar los proyectos de investigación universitarios que contengan datos personales accesibles a través de redes de telecomunicaciones.
11.5. Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.	• Instalar herramientas de hardware o software que ayuden a una gestión eficaz de la seguridad y los compromisos u obligaciones legales de la organización en el área de la protección de datos personales. • En el caso de que pudiera resultar necesario, instalar herramientas de detección de intrusiones (IDS o Intrusion Detection Systems) y/o de prevención de intrusiones (IPS o Intrusion Prevention Systems) con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad. • En la medida que pudiera resultar necesario, implantar sistemas de Prevención de Pérdida de Datos (DLP o Data Loss Prevention) con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad.
11.6. Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.	• Establecer mecanismos de registro de acciones sobre los datos personales o logging así como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes.
11.7. Uso de identificadores que revelan información del afectado. Deficiencias en la protección de la confidencialidad de la información.	• Establecer políticas de asignación de códigos de usuario por parte de la organización que eviten datos triviales como fecha de nacimiento, nombre y apellidos, etc. • Evitar el uso de identificadores ligados a elementos de autenticación, como números de tarjetas de crédito o similares, ya que favorecen el fraude en la identificación e incluso la suplantación de identidad.
11.8. Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.	• Establecer políticas y acciones formativas encaminadas a hacer llegar a los miembros de la organización las normas de seguridad aplicadas en la misma.

11.9. Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados.	• Aplicar políticas de seguridad globales para frenar los posibles ataques generados por este motivo.
11.10. Defectos en las capacidades de resiliencia de la entidad.	• Implementar políticas adecuadas de backup de los datos.
11.11. Defectos en las condiciones de seguridad en el almacenamiento de los datos de la organización.	• Implementar políticas adecuadas de cifrado de los datos.
11.12. Defectos en las condiciones de seguridad en el acceso a los datos de la organización.	• Implementar políticas adecuadas de cifrado en las comunicaciones.

Anexo 5. Cuestionario valoración metodología de gestión de protección de datos personales en colectivo investigadores universitarios.

Datos generales investigador.

- Doctor: Si ☐ No ☐ Doctorando ☐
- Indicar el área o áreas de conocimiento:
- Participación en investigación con datos de carácter personal: Si ☐ No ☐

Valoración metodología.

Valore (en un rango de 0 a 9, siendo 0 la puntuación más baja y 9 la más alta) la metodología propuesta, de forma global.

  - (01) Grado de documentación de la metodología:
  - (02) Grado de comprensión general:
  - (03) Grado de complejidad de uso:
  - (04) Grado de posible mejora para el investigador en la gestión de proyectos con datos personales:

Valore (en un rango de 0 a 9, siendo 0 la puntuación más baja y 9 la más alta) las distintas características de la metodología propuesta.

- Fase 0. Verificación de la existencia de tratamientos de datos personales e identificación de la fuente de los mismos.
  - (05) Grado de documentación de la fase:
  - (06) Grado de comprensión general:
  - (07) Grado de complejidad de uso:
- Fase 1. Identificación de los tratamientos.
  - (08) Grado de documentación de la fase:
  - (09) Grado de comprensión general:
  - (10) Grado de complejidad de uso:
- Fase 2. Identificación de riesgos y clasificación del proyecto.
  - (11) Grado de documentación de la fase:
  - (12) Grado de comprensión general:
  - (13) Grado de complejidad de uso:
- Fase 3. Revisión del sistema de información al interesado, obtención del consentimiento y clausulado en formularios.
  - (14) Grado de documentación de la fase:
  - (15) Grado de comprensión general:
  - (16) Grado de complejidad de uso:
- Fase 4. Implementación del ejercicio de derechos por parte de los interesados.

  - (17) Grado de documentación de la fase:
  - (18) Grado de comprensión general:
  - (19) Grado de complejidad de uso:

- Fase 5. Aplicación de medidas de seguridad (investigadores y universidad).
  - (20) Grado de documentación de la fase:
  - (21) Grado de comprensión general:
  - (22) Grado de complejidad de uso:

- Fase 6. Aplicación de anonimización y seudonimización.
  - (23) Grado de documentación de la fase:
  - (24) Grado de comprensión general:
  - (25) Grado de complejidad de uso:

- Fase 7. Análisis de las implicaciones de los tratamientos.
  - (26) Grado de documentación de la fase:
  - (27) Grado de comprensión general:
  - (28) Grado de complejidad de uso:

Valore (en un rango de 0 a 9, siendo 0 la puntuación más baja y 9 la más alta) las siguientes características de las plantillas proporcionadas por la metodología:

- Plantilla Identificación de tratamiento de datos personales (Anexo 1).
  - (29) Grado de documentación de la plantilla:
  - (30) Grado de comprensión general:
  - (31) Grado de complejidad de uso:

- Plantilla Identificación de riesgos en los tratamientos de datos personales (Anexo 2).
  - (32) Grado de documentación de la fase:
  - (33) Grado de comprensión general:
  - (34) Grado de complejidad de uso:

- Plantilla Documento estándar de Consentimiento Informado (Anexo 3).
  - (35) Grado de documentación de la fase:
  - (36) Grado de comprensión general:
  - (37) Grado de complejidad de uso:

- Catálogo general de amenazas y posibles soluciones, aplicable a los tratamientos de datos personales (Anexo 4).
  - (38) Grado de documentación de la fase:
  - (39) Grado de comprensión general:
  - (40) Grado de complejidad de uso:

Sugerencias de mejora.

Enumerar las posibles sugerencias de mejora para la metodología propuesta.