Universidad de Alcalá

GUÍA DE PROTECCIÓN DE DATOS EN INVESTIGACIÓN de la UNIVERSIDAD DE ALCALÁ

UNIDAD DE PROTECCIÓN DE DATOS

Versión 1.0

Junio de 2024

ÍNDICE

1. INTRODUCCIÓN - ÁMBITO DE APLICACIÓN DE LA GUÍA

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. Además, entre otras normas internacionales y supranacionales, el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

Pero, en una investigación –sea cual sea: TFG, TFM, Tesis Doctoral o Proyecto de investigación-, no sólo se debe tener en cuenta el cumplimiento de la legalidad de esta Protección de datos de carácter personal regulada por la normativa promulgada al respecto, sino que se debe actuar con responsabilidad y concienciación de que se está trabajando con datos de personas que están participando en tu investigación y han depositado en ti/vosotros esa confianza.

> *Ten en cuenta que …*
>
> *Hay que colaborar en la materialización de la cultura institucional de la protección de los datos personales. Se debe interiorizar la lógica de la normativa en la materia. Y concienciarnos de la promoción de la tutela de los datos personales (de las personas físicas).*

Antes de pasar a desarrollar el contenido de esta Guía, queremos indicar cuál es la legislación básica tanto nacional como europea en la que se basa la Protección de datos, así como indicar la página web de la Agencia Española de Protección de Datos, en donde encontraréis mucha de la documentación citada esta Guía:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos (LOPDGDD)
- 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) (RGPD)
- Agencia Española de Protección de Datos (AEPD)

También es importante indicar aquí, antes de pasar a desarrollar el contenido de esta Guía, cuáles son los **Principios relativos a la Protección de datos**, por considerarlos fundamentales para llevar a cabo cualquier tratamiento de datos personales, que iremos viendo a lo largo de la misma:

- Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado («**licitud, lealtad y transparencia**»), es decir, proporcionando toda la información relativa al tratamiento de sus datos, y recabando su consentimiento expreso.
- Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con los fines que motivaron la recogida («**limitación de la finalidad**»).
- Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («**minimización de datos**»).
- Los datos personales serán exactos y, si fuera necesario, actualizados («**exactitud**»).
- Los datos personales serán mantenidos de forma que se permita la identificación de las personas interesadas durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en todo caso, siempre protegiendo los derechos y libertades de la persona interesada («**limitación del plazo de conservación**»).
- Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («**integridad y confidencialidad**»).

> *Principios relativos a la protección de datos: Licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; e integridad y confidencialidad.*

Esta Guía seguirá las preguntas realizadas en el **"Cuestionario sobre el tratamiento de datos personales en Proyectos de Investigación, Tesis, TFM y TFG en la UAH"** con la intención de ayudar, de esta forma, a contestar dicho formulario. Estas son las cuestiones a las que tenéis que responder al diseñar un proyecto, antes de poner en marcha vuestra actividad de investigación, si vais a necesitar datos de personas.

Pero antes de ir respondiendo a las preguntas del Cuestionario, esta Guía ofrecerá en primer lugar, para que os sea más fácil su cumplimentación, algunas definiciones y conceptos importantes en cuanto a la protección de datos se refiere, que vais a utilizar en vuestra actividad de Investigación, ya sea un Proyecto de investigación, una investigación básica, aplicada o tutelada como tesis doctoral, trabajos fin de máster o trabajos fin de grado.

VOLVER AL INICIO DEL DOCUMENTO

2. CUESTIONARIO SOBRE EL TRATAMIENTO DE DATOS PERSONALES EN PROYECTOS DE INVESTIGACIÓN, TESIS, TFM Y TFG EN LA UAH o *20 PREGUNTAS BÁSICAS PARA ORGANIZAR TU PROYECTO DE INVESTIGACIÓN*

1. ¿Cómo se llama tu actividad de investigación?
2. ¿Cuál es el objetivo de tu investigación? ¿Cuál es su finalidad?
3. ¿Necesitas que algunas personas te proporcionen sus datos personales para llevar a cabo tu investigación?
4. ¿Qué tipo de datos concretos necesitas?
5. ¿Con qué fin, desde el punto de vista metodológico, necesitas esos datos?
6. ¿Cómo obtendrás esos datos? ¿directamente de las personas donantes o participantes en tu investigación?
7. ¿A través de qué mecanismos (encuesta, entrevista, historia clínica) vas a extraer y recoger los datos de las personas participantes?
8. ¿Has elaborado un documento con información concreta, suficiente y veraz para explicarles lo que vas a pedirles a las personas donantes y para qué vas a utilizar esa información?
9. ¿Has incluido en el documento la información sobre cuáles son sus derechos y la posibilidad de que los ejerzan?
10. Si te proporcionan los datos otras fuentes que no son las personas donantes ¿cómo lo harán? ¿Quiénes?
11. ¿Quiénes intervienen en tu trabajo de investigación? ¿Te ayuda/n otra/s persona/s, alguna ONG o empresa externa? ¿Existe algún vínculo con ellos, contrato o convenio firmado?
12. ¿Vas a colaborar con otros grupos de investigación, entidades o personas que están fuera de la Unión Europea? ¿De qué países son o dónde están? ¿Existe algún vínculo con ellos, contrato o convenio firmado?
13. ¿Dónde vas a guardar los datos y a trabajar con ellos, mientras dure tu investigación?
14. ¿Quiénes van a poder acceder y usar los datos para llevar a cabo el trabajo de investigación?
15. ¿Cuánto tiempo vas a necesitar trabajar con esos datos y conservarlos después? ¿Cómo tienes previsto destruir los datos una vez finalizado su tiempo de conservación?
16. ¿Cuándo tengas los datos, los seudonimizarás haciendo una separación de los datos y las identidades con códigos, para evitar la identificación personal?

17. ¿Has realizado un Análisis de riesgos? Y si fuese necesario, ¿has realizado una Evaluación de Impacto?
18. ¿Cómo vas a garantizar la seguridad de la información? Para ello, tendrás que hacerte las siguientes preguntas: ¿Qué perjuicios podría suponer para las personas que te han donado sus datos que se te perdieran o que alguien los usara ilícitamente? ¿Qué perjuicios supondría para la investigación que no pudieras acceder a los datos recogidos? ¿Qué mecanismos has previsto para que no los usen ilícitamente?, ¿y para que no se te extravíen?, ¿o para que no se te bloquee el acceso?
19. ¿Tienes previsto ceder los datos a personas ajenas a tu equipo de investigación?
20. ¿Tienes preparado algún documento para registrar todo lo que estás haciendo en relación con la protección de la información recogida para tu investigación?

VOLVER AL INICIO DEL DOCUMENTO

3. ¿QUÉ ES UN DATO PERSONAL?

Un dato personal es cualquier *información* numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo sobre personas físicas identificadas o identificables. Las informaciones que hacen identificable a alguien son aquellas sobre su identidad física, fisiológica, económica, cultural, política, educativa, religiosa, etc. que permiten saber quién es la persona de la que procede la información.

Ten en cuenta que …

No es sólo el nombre y apellidos o el DNI, por ejemplo. Dato personal también son la imagen, el correo electrónico, las calificaciones, los datos de salud, de afiliación política o sindical, y etnia o raza, entre otros atributos.

3.1. FINALIDAD Y PROCEDENCIA

Al diseñar la futura investigación (Proyecto de Investigación, Tesis doctoral, TFM, TFG) tienes que tener muy claro *por qué* y *para qué* recoges los datos, los registras, los estudias, los conservas, etc. y también que no puedes tratarlos posteriormente de manera incompatible –de modo diferente– con dichos fines, puesto que los datos personales siempre tienen que ser tratados con una finalidad concreta, explícita y legítima.

También has de tener en cuenta el *principio de minimización* de datos: sólo debes recoger los datos imprescindibles para llevar a cabo la investigación, pero no recojas más datos o distintos a los que estaban contemplados en el diseño inicial del proyecto o "por si acaso hacen falta más adelante".

Lógicamente también necesitas prever y dejar constancia en tu proyecto de dónde extraerás esa información (directamente de la persona donante, de diversos documentos del tipo historia clínica, informes u otras fuentes indirectas).

Recuerda que …

No debes utilizar los datos personales recabados para una finalidad distinta a la inicialmente prevista en el momento de recoger la información. Y no hay que solicitar datos que estén en la esfera de lo privado, si no son realmente útiles a nuestra investigación.

En el siguiente cuadro mostramos, de forma resumida, las finalidades del tratamiento de los datos personales que vas a realizar y de dónde proceden dichos datos.

LAS 5W SOBRE FINALIDADES Y PROCEDENCIAS

WHAT/qué: Describe con precisión la información o tipo de datos que necesitas recoger.

Principio de minimización de datos: sólo se recogen los datos imprescindibles.

WHY/por qué: Expón claramente con qué fines los recoges, registras, estudias, analizas, cruzas, conservas, etc.

Límites de la finalidad: no puedes tratarlos posteriormente de manera incompatible con esos fines.

WHERE/dónde: Especifica de dónde los recoges; si directamente de donante, de documentos tipo historia clínica, informes, expedientes o de otras fuentes indirectas y si será por medio de entrevistas, encuestas, test, fichas, etc. *Confidencialidad.*

WHO/quién: Recoge qué perfil de personas voluntarias serán donantes y quiénes haréis cada tratamiento.

WHEN/cuándo: Ordena los tiempos de cada paso: recogida, *pseudonimización*, conservación, transferencia, etc.

3.2. CATEGORÍAS DE PERSONAS INTERESADAS

La legislación llama «personas interesadas» a aquellas que te dan sus datos y que tú transformarás en información para tu actividad de investigación.

En realidad, estas personas interesadas son las personas donantes o que tú has reclutado para que participen en la actividad de investigación. Son aquellas *personas reclutadas* a las que, una vez que les has explicado para qué las necesitas, con qué fines y en qué manera utilizarás y protegerás sus datos personales, te ceden esa información que les has solicitado.

Recuerda que …

La persona encuestada, entrevistada, grabada, fotografiada, etc., está cediendo sus datos y es "persona interesada" en la protección de su información personal.

3.3. CATEGORÍAS ESPECIALES DE DATOS

Hay datos, que puedes necesitar para la investigación y, que por su relevancia para la privacidad de las personas donantes tienes que tratar con mayor cuidado, y cumpliendo una serie de requisitos. No todos los datos de carácter personal son iguales y la normativa los clasifica de la siguiente manera:

3.3.1. DATOS SENSIBLES O ESPECIALMENTE PROTEGIDOS

Se trata de una categoría de datos que, debido a *su incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona donante*, hace necesario que establezcas una mayor protección que con el resto de los datos personales (RGPD Art. 9 y Considerandos 51-56).

Estos datos son, sin ánimo de exhaustividad, los relativos a:

- Ideología u opiniones políticas
- Afiliación sindical
- Religión u opiniones religiosas
- Creencias o creencias filosóficas
- Origen racial o étnico
- Datos relativos a la salud
- Vida sexual u orientación sexual e identidad de género
- Violencia de género y agresión sexual
- Datos genéticos
- Datos biométricos
- Datos relativos a condenas y delitos penales
- Datos relativos a sanciones administrativas

En las actividades de investigación universitarias, y de otros centros, es frecuente utilizar todo tipo de datos sensibles, dado que se investiga en ciencias biológicas, biomédicas, técnicas, sociales, jurídicas y de la conducta. Pero son especialmente delicados:

a) Datos relativos a la **salud**. Todos aquellos que revelan información sobre el estado de salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria. De hecho, son datos de salud las informaciones relativas a enfermedad, discapacidad, riesgo de padecer enfermedades, tratamientos clínicos, estado fisiológico o biomédico, etc.,

independientemente de que la fuente sea su historia clínica o un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro, o incluso información transmitida por el propio participante en la actividad de investigación.

Ten en cuenta siempre que, para los tratamientos de recogida, uso, conservación, etc. que vayas a hacer de esta información, la normativa en protección de datos se complementa, entre otras muchas, con la Ley de Autonomía del Paciente 41/2002, que regula los derechos y obligaciones en materia de información y documentación clínica, incluyendo la comunicación, la toma de decisiones, el consentimiento informado, el acceso a la historia clínica, etc.

b) Datos **genéticos**. Datos específicos de salud que identifican la información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos.

c) Datos **biométricos**. Informaciones sobre las características físicas, fisiológicas o conductuales de una persona, obtenidas con técnicas específicas como imágenes faciales, datos dactiloscópicos, etc. que permiten o confirman la identificación única de dicha persona (RGPD. Art. 4.14).

Más información al respecto en la Agencia Española de Protección de Datos (AEPD), en su Sección sobre SALUD, en el epígrafe "Investigación sanitaria y ensayos clínicos".

3.3.2. DATOS DE MENORES

En principio no son *datos sensibles*, pero en la normativa se enuncia que debido a su condición de vulnerabilidad tienes que tratarlos como tales, ya que estas personas pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes a la recogida y la utilización de sus datos personales, y es responsabilidad tuya evitar que sean vulnerados.

A modo orientativo considera que si los datos que vas a solicitar pueden generar al menor alguna tensión grave o afectación se consideraría una investigación invasiva y tendrás que pedir consentimiento a los representantes legales (progenitores o tutores) y asegurarte de que a partir de los 12 años el menor asiente. Cuando los datos no son de ese tipo, entonces sólo necesitarás la autorización de los representantes legales en los menores de 14 años y su

asentimiento, a partir de esta edad -mayores de 14 años- son ellos los que consienten o no por sí solos.

En el caso de que solo se pueda conseguir el consentimiento de uno de los representantes legales (progenitores o tutores), resulta conveniente que éste se responsabilice del consentimiento del otro representante legal del menor.

No obstante, existen supuestos en los que la edad para consentir el tratamiento o la cesión de datos es superior a los 14 años, como puede ser el caso de estudios de investigación biomédica, en donde, *"Conforme al RGPD y a la LOPDGDD, el consentimiento para el tratamiento de datos personales se ha de prestar por los propios interesados o por sus representantes legales. Para los menores de edad, pero mayores de 14 años se requerirá igualmente el consentimiento de padres o tutores cuando la Ley exija la asistencia de los padres y tutores, así como para los mayores de edad que estén sometidos a tutela"* (AEPD).

Además, está prohibido cualquier tratamiento o cesión de datos y/o imágenes de un menor que atente, de manera objetiva, contra su honor, intimidad y propia imagen. En estos casos, la obtención del consentimiento del propio menor o de sus representantes legales no sirve para legitimar dicha intromisión ilegítima.

> *Para obtener más información al respecto en la Agencia Española de Protección de Datos (AEPD), en su infografía "Información sobre consentimiento para tratar datos personales de menores de edad" y en su Sección de FAQs "Menores y educación".*

3.3.3. DATOS DE PERSONAS DE COLECTIVOS EN SITUACIÓN DE ESPECIAL VULNERABILIDAD

Es preciso que tengas un cuidado especial si la actividad de investigación implica el uso de datos de personas de colectivos en situación de especial vulnerabilidad, como menores (ya citados), personas discapacitadas, ancianas, con riesgo de exclusión social, en situaciones políticas comprometidas, situación administrativa irregular, etc.

VOLVER AL INICIO DEL DOCUMENTO

4. TRATAMIENTO DE DATOS PERSONALES

Se denomina "tratamiento de datos" a cualquier operación o conjunto de ellas que realices sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no. También se considera tratamiento de datos aquella utilización de datos que, sin ser personales, su agrupación identifica o hace identificable a una persona.

Así, son tratamientos (uso) de datos 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 de dichos datos. También son tratamiento de datos la seudonimización o la anonimización, codificación o disociación, la conservación de los documentos escritos de consentimiento informado, etc.

En una actividad de investigación puedes tener que incluir uno o varios tratamientos de datos personales distintos. Además de tratar los datos necesarios de las personas para llevar adelante la investigación, siempre vas a tener que "tratar" la información sobre los miembros de tu propio equipo investigador (datos personales) aunque este no sea un tratamiento de datos para la investigación.

Debéis tener en cuenta que la definición de tratamiento de datos de datos personales que nos da la legislación en materia de Protección de datos es distinta a la que se usa de manera habitual o coloquial y puede llevar a confusión –que implicaría problemas jurídicos, de mayor o menor gravedad–. Generalmente para la persona investigadora el tratamiento de datos en una actividad científica suele referirse al *método estadístico o de análisis* empleado para extraer conclusiones a partir de los datos obtenidos en los experimentos, realizados en el laboratorio, en las muestras, en los trabajos de campo o en cualquier otro ámbito en el que se esté aplicando la metodología propia de cada disciplina científica, mientras que en la regulación normativa de Protección de datos, el tratamiento de los mismos, como se ha comentado en párrafos anteriores, puede ser sólo la recogida de los datos personales.

Los derechos y libertades fundamentales de las personas interesadas pueden ser vulnerados o lesionados cuando el tratamiento de sus datos personales es inadecuado, ya sea porque las personas responsables del tratamiento omiten –o ignoran deliberadamente– las medidas técnicas u organizativas que la normativa nacional y europea establece para realizar dicha protección.

*La AEPD define una **brecha de seguridad** como "un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales".*

VOLVER AL INICIO DEL DOCUMENTO

5. RESPONSABLE DEL TRATAMIENTO

El **Responsable del Tratamiento** es la persona física o jurídica que se responsabiliza del tratamiento o tratamientos de los datos, y que tiene que estar siempre identificada. En nuestro caso, la Universidad de Alcalá sería la responsable, recayendo dicha responsabilidad en la Secretaría General.

En toda investigación, el responsable de los tratamientos de la investigación es la persona investigadora principal, tutora o directora de tesis, TFMs, TFGs, y tiene la consideración de responsable interna del tratamiento a efectos prácticos, pero es siempre la Universidad de Alcalá la Responsable de todos los tratamientos con datos personales que tengan lugar en la institución universitaria.

> *Ten en cuenta…*
>
> *El Responsable último del tratamiento de datos personales en la UAH es, con carácter general, la Secretaría General. Sin perjuicio de la responsabilidad que se asume en la práctica al tratar información personal en el marco de una investigación específica.*

Cuando, como responsable de la investigación, necesites la ayuda de los servicios de una persona o de una entidad externa a la UAH que trate los datos personales, siempre deberá hacerse bajo tus instrucciones como, por ejemplo, una empresa de servicios informáticos, y a esta persona o empresa se le llama **Encargado del Tratamiento**.

La relación existente con estas personas físicas o jurídicas puede hacerse mediante Contrato o Convenio. Pero, además, hay que firmar, entre las Partes, un *Contrato o Acuerdo de tratamiento de datos personales* o más conocido como Acuerdo de Confidencialidad.

> *Encontrarás información útil sobre cómo formalizar tu relación con el Encargado del tratamiento de datos, con sugerencia de modelos, en el apartado "Documentación UAH - Modelos" de la web de Protección de Datos*

VOLVER AL INICIO DEL DOCUMENTO

6. DELEGADA DE PROTECCIÓN DE DATOS

La Delegada de Protección de Datos (DPD) —en inglés, Data Protection Officer (DPO)— es una persona con conocimientos en protección de datos que las Universidades públicas y privadas, así como otras instituciones, están obligadas a designar.

La DPD se encarga de informar, asesorar, ayudar y responder a todas las consultas sobre protección de datos de la entidad responsable (en nuestro caso la UAH) y también del responsable interno del tratamiento (en el campo de la investigación quien asuma el rol de IP o la persona designada por el equipo investigador).

La DPD tiene que asegurase de que se cumplan las obligaciones legales en materia de protección de datos, también velando y cooperando con la Autoridad de Control (Agencia Española de Protección de Datos, AEPD), siendo la interlocutora y punto de contacto entre la UAH y la AEPD.

La Universidad deberá proveer a la DPD de los recursos humanos y materiales necesarios para el desempeño de sus funciones. Por ello, se creará a tal efecto una Unidad o Servicio, que estará bajo su dirección y contará con el personal que resulte necesario.

En estos momentos, la DPD de la Universidad es miembro del Comité de Ética en la Investigación (CEI) e informará sobre tu proyecto en materia de protección de datos, por lo que la relación entre tus tareas de investigación con datos personales y su trabajo como DPD es obligada y directa.

Como investigador/a has de ponerte en contacto con la DPD o con la Unidad de Protección de Datos cuando tengas alguna duda sobre el tratamiento de datos personales en tu investigación y no puedas resolverla leyendo esta Guía y/o el material publicado en las webs de Protección de datos y del Comité de Ética de la UAH.

Los datos de contacto de la Unidad de Protección de Datos son: protecciondedatos@uah.es y 91885- 6473 - 6476 - 6453.

Más información en https://www.uah.es/protecciondedatos

VOLVER AL INICIO DEL DOCUMENTO

7. LICITUD DEL TRATAMIENTO DE LOS DATOS

La **licitud del tratamiento de los datos** quiere decir sencillamente que debes cumplir con las condiciones necesarias para que el tratamiento de datos personales que se realicen en tu investigación sea legítimo (bien hecho y legalmente seguro).

La licitud del tratamiento es lo que también se llama "base jurídica", y es la que permite tratar datos en tu actividad de investigación: una vez que se han identificado los datos que se van a recoger, de quiénes y el tratamiento que se les va a dar, sólo será legítimo que se haga todo ello si se dispone del *consentimiento informado* de las personas donantes, que han de otorgar el consentimiento de manera libre, específica, explícita e inequívoca para todos los fines que vayas a utilizarlos (Art. 6 LOPDGDD).

Otras bases jurídicas para el tratamiento de datos como son la *obligación legal*, el *interés público* o el *ejercicio de poderes públicos,* en el ámbito de la investigación con seres humanos no restan valor ni sustituyen al deber de información y de consentimiento que se tiene, sólo reflejan algunas situaciones en las que la persona donante conoce que existe un interés público (Art. 8 LOPDGDD y Art. 9 RGPD).

> *El consentimiento debe ser inequívoco. Esto es, que se preste a través de una manifestación de la persona interesada o mediante una clara acción afirmativa. Queda excluido el llamado "consentimiento tácito" (casillas ya marcadas o la inacción, por ejemplo). Lo adecuado sería, por ejemplo, la utilización de una declaración por escrito o la marcación de un check en un sitio web de internet.*

> *En los supuestos de datos sensibles, adopción de decisiones automatizadas o transferencias internacionales, además de inequívoco, el consentimiento deberá ser explícito.*

En el Apartado 9 de esta Guía se tratará el tema del Consentimiento con más detalle.

Condiciones generales y requisitos para legitimar el tratamiento de datos sensibles

Por regla general, se prohíbe la recogida, el uso o almacenamiento -es decir, el tratamiento- de datos sensibles o especialmente protegidos, pero puedes tratar los datos sensibles para tu investigación si cumples una o más de las condiciones siguientes:

- Tienes el *consentimiento explícito* del interesado/donante para una *finalidad de*

actividad de investigación específica.

- Son datos necesarios con fines de archivo e interés público, *fines de investigación científica o histórica o fines estadísticos* y están *seudonimizados* por otros.
- Hay razones de *interés público en el ámbito de la salud pública.*

Y tienes que cumplir los siguientes requisitos:

1. Obtén el *consentimiento explícito* por escrito de las personas reclutadas que confirme que acceden a darte sus datos, para qué servirán y cómo se tratarán.
2. Asegúrate de la calidad de esa información, es decir que son *datos adecuados, veraces y pertinentes* para tu investigación, ponderando la necesidad de los mismos. Es decir, valorando si todos los datos que vas a recoger son realmente indispensables para llevar a cabo la actividad de investigación. Si no son necesarios para la realización de la actividad de investigación, no hay que pedir esos datos personales (criterio o principio de minimización de datos).
3. Asegúrate también de que la recogida no se hace de forma desleal, fraudulenta o ilícita.
4. No olvides que en el caso de que recojas datos de salud para tu investigación, debes facilitar cualquier información que obtengas relacionada con la salud del donante que le sea útil.
5. Realiza un *juicio de proporcionalidad* entre la finalidad científica que persigues y el medio que vas a utilizar.
6. Cuando necesites para tu investigación datos de salud procedentes de la historia clínica de la persona interesada recoge siempre una hoja o *documento de información* y consentimiento que incluya:
    a) Nombre del profesional y del centro donde ha sido atendido el paciente.
    b) Propósitos de la petición.
    c) Expresa conformidad de publicación del caso clínico en publicaciones científicas dirigidas a profesionales de la salud.
    d) Nombre del paciente.
    e) Documento de identidad o pasaporte y su firma autorizando expresamente que se utilicen los datos de su historia clínica en las condiciones que se describen en el informe.
7. Asegúrate del cumplimiento del compromiso de confidencialidad por parte de las personas que tienen acceso a los datos, incluso cuando la relación que vincule a las partes ya haya finalizado.

    Hay que tener en cuenta lo indicado en el Código Penal:

Art 199: 1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses. 2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Circunstancias especiales de uso legítimo en investigación en salud

En las investigaciones relacionadas con la salud, especialmente en biomedicina, hay dos circunstancias especiales en las que podrás utilizar los datos personales con legitimidad:

1. Cuando la finalidad o el área de investigación esté relacionada con aquella para la que se obtuvo el consentimiento de la persona interesada; por ejemplo, el consentimiento lo prestó para el tratamiento de datos de investigación de un determinado tipo de cáncer y los quieres seguir tratando para investigación oncológica general. Entonces, tienes que *informar a los afectados* y necesitas un *informe previo favorable del Comité de Ética de Investigación (CEI).*
2. Los datos han sido *seudonimizados* por otro equipo con el consentimiento de las personas reclutadas para dicho tratamiento. Hay que asegurarse de la existencia del *compromiso de confidencialidad* y de que *no se producirá la reidentificación*.

La Disposición Adicional Decimoséptima de la LOPDGDD introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

VOLVER AL INICIO DEL DOCUMENTO

8. DEBER DE INFORMAR

Como investigador/a debes facilitarles, a quienes participen en tu investigación dándote sus datos personales, toda la información necesaria que les diga para qué –la finalidad de tu investigación- y cómo se tratarán sus datos, incluyendo en dicha información la posibilidad de ejercer sus derechos. Y debes hacerlo con un lenguaje claro y sencillo: de forma concisa, transparente, inteligible y de fácil acceso.

Ten en cuenta…

La persona investigadora tiene que informar a las personas que dan sus datos personales, de manera sencilla (clara y fácil) y accesible: con qué finalidad investigo, cómo trataré los datos, y qué derechos puede ejercer ante la UAH.

8.1. ¿QUIÉN TIENE QUE INFORMAR Y CUÁNDO?

La obligación de informar a las personas donantes de sus datos recae sobre la persona *responsable* interna de la investigación, que será el IP o la designada por ella. Este responsable tiene que informar, en nombre de la Universidad de Alcalá, ya que, como se ha dicho, es la Responsable del tratamiento.

Debes tener en cuenta que toda la información se debe poner a disposición de los posibles donantes de datos personales con **anterioridad** a la recogida de los datos.

8.2. EXCEPCIONES A LA OBLIGACIÓN DE INFORMAR

No es necesario que informes cuando:

- La persona donante o participante en tu investigación ya disponga de la información.
- Es *imposible* informar o supone un *esfuerzo desproporcionado*, en cuyo caso tendrás que tomar medidas adecuadas y concretas para proteger sus derechos.

8.3. ¿CUÁL SERÁ EL CONTENIDO DE LA INFORMACIÓN APORTADA?

Las características de una buena información siempre son la sencillez, la claridad, la concisión, la transparencia, la inteligibilidad y el fácil acceso.

La información que debe ofrecerse tendrá que contener: la finalidad para la que se tratan los datos, la base legítima de dicho tratamiento, si existe o no cesión de datos, si existe o no transferencia internacional de datos, el tiempo de conservación de los mismos, quién es el Responsable del tratamiento, ante quién se podrán ejercer los derechos, y qué hacer y a quién acudir en caso de que exista un conflicto con la Universidad de Alcalá.

La información que se muestre siempre tiene que ser veraz, precisa, clara y comprensible.

Cuando estamos tratando datos personales de niños o de personas con carencias sociales, educacionales o de cualquier otro tipo, la información que les ofrezcamos, además de tener las características ya enumeradas, debería ser acorde a su edad y sus circunstancias particulares, reiterando que el lenguaje utilizado debe ser claro y sencillo, que sea fácil de entender.

8.4. ¿CÓMO INFORMAR?

Para informar correctamente debes adaptar adecuadamente la información al modelo de recogida de datos que vayas a utilizar:

- Formularios en papel.
- Formularios en la web.
- Entrevista telefónica o presencial.

En el mismo documento donde pidas el consentimiento, también puedes informar sobre la investigación para la que le pides su participación, y sobre los datos personales que le solicitas para realizarla.

Recuerda que …

Junto con la solicitud del consentimiento se puede dar la información, en el soporte que creas más adecuado, sobre la finalidad del tratamiento de sus datos personales, así como la base (jurídica) que lo legitima, si se van a ceder los datos, si existirá transferencia internacional de datos, cuánto tiempo se van a conservar los datos, quién es responsable del tratamiento, ante quién puede ejercer sus derechos ARSOPOL, y cómo solucionar un posible conflicto con la UAH. Todo ello, teniendo en cuenta la edad y/o circunstancias personales de quienes obtendremos los datos.

8.5. CUSTODIA

Recuerda que el cumplimiento diligente de la protección de datos te obliga a guardar un justificante de que has informado, por ello, debes guardar, en el soporte más apropiado, el justificante de que lo has hecho.

Los documentos con la información y los consentimientos expresos firmados por las personas participantes en tu investigación, se tienen que guardar para tener constancia de las acciones llevadas a cabo, y poder demostrar que se han realizado, por si fuera necesario mostrarlo ante la Autoridad de Control competente, si ésta lo exigiera. Además, se debe dar una copia a las personas participantes de todo lo que firmen, incluida la información facilitada sobre el tratamiento a llevar a cabo, y tener en cuenta que dichas personas participantes pueden revocar dicho consentimiento cuando lo deseen, y entonces, se deberán de dejar de tratar sus datos en ese momento, aunque no se suprimirán los resultados ya obtenidos.

8.6. INFORMACIÓN SOBRE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, OPOSICIÓN, PORTABILIDAD DE LOS DATOS, DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS Y LIMITACIÓN DEL TRATAMIENTO (ARSOPOL)

Con la información sobre los derechos siempre se trata de promover la *capacidad de decisión y de control* que la persona interesada tiene sobre sus propios datos personales. Por ello, como responsable de la investigación, tienes que informar a la persona donante o participante en tu investigación sobre sus derechos, sobre

cómo puede ejercerlos y cuál será la forma de ponerse en contacto con la Universidad para hacerlo. Para ello, en la página web de la Unidad de Protección de Datos https://www.uah.es/protecciondedatos hay un apartado llamado "Solicitudes. Ejercita tus Derechos" donde se encuentra el Procedimiento para ejercitar los derechos y cada una de las distintas solicitudes, dependiendo del derecho que se quiera ejercitar. También se podrán ejercer los distintos derechos ARSOPOL a través de la Sede electrónica de la UAH – Catálogo de trámites – Solicitud para ejercitar los Derechos a la Protección de Datos.

Los derechos ARSOPOL son:

- Derecho de **A**cceso o derecho a solicitar información al responsable sobre si sus datos están siendo tratados y, en caso afirmativo, qué datos son los tratados.
- Derecho de **R**ectificación o derecho a solicitar la modificación de datos que sean inexactos o incompletos.
- Derecho de **S**upresión o derecho a solicitar la supresión de los datos en determinados supuestos, pero no se suprimirán los resultados ya obtenidos.
- Derecho de **O**posición o derecho a oponerse al tratamiento de sus datos personales por motivos relacionados con su situación particular.
- Derecho a la **P**ortabilidad de los datos o derecho a solicitar que se le faciliten los datos en un formato estructurado, de uso común y lectura mecánica y el derecho a transmitirlos a otro responsable.
- Derecho a no ser **O**bjeto de Decisiones individuales automatizadas o derecho a que las personas participantes no sean objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de perfiles, que les pueda producir efectos jurídicos o que les afecte significativamente de forma similar, como sería la evaluación de aspectos personales, como su rendimiento en el trabajo, situación económica, salud, las preferencias o intereses personales, fiabilidad o su comportamiento.
- Derecho a la **L**imitación del tratamiento o derecho a solicitar que se limite el tratamiento de sus datos en determinadas condiciones.

Recuerda …

Derechos ARSOPOL: Acceso, Rectificación, Supresión, Oposición, Portabilidad de los datos, Derecho a no ser objeto de decisiones individuales automatizadas, y Limitación del tratamiento.

8.7. INFORMACIÓN SOBRE EL TIEMPO DE CONSERVACIÓN DE LOS DATOS

Debes informar sobre el tiempo de conservación de los datos, indicar a la posible persona donante que el plazo mínimo de conservación es con carácter general de *cinco años*, con fines de auditoría y verificación de la investigación realizada con esos datos, con algunas matizaciones que se verán más adelante. También le informarás de que puedes conservar los datos recogidos para la investigación mientras no solicite su *supresión* y esos datos sigan respondiendo a la finalidad para la que fueron obtenidos. Y, además, que no podrá pedirte que suprimas los resultados obtenidos con sus datos hasta el momento previo a la solicitud de supresión.

Tanto el Reglamento Europeo de Protección de Datos (RGPD) como la Ley de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) no indican un plazo de conservación determinado, sino que establecen que este plazo será el estrictamente necesario para cumplir con la finalidad para la que los datos personales fueron recogidos («**Principio de conservación**»).

La legislación indica que los datos podrán conservarse durante periodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos -por lo que también podrían conservarse durante más tiempo (sin especificar en la legislación, tampoco plazo concreto) por tratarse de una investigación científica-, y podrían destruirse los datos cuando finalice el proceso de edición, garantizando durante ese plazo las adecuadas medidas de custodia de los datos.

Ten en cuenta …

Hay que informar sobre el plazo de conservación de los datos, acorde con su finalidad, pero no siempre existe una duración señalada expresamente en la normativa aplicable. En el caso de la investigación científica se podría prolongar el plazo hasta finalizar, por ejemplo, la publicación o difusión de los resultados de la investigación. Lo más importante es garantizar las adecuadas medidas de seguridad de conservación de los datos, con técnicas como la anonimización, entre otras apropiadas para custodiar correctamente la información personal de las personas participantes.

Se ampliará la información sobre el tiempo de conservación de los datos en el Apartado 12 de esta Guía.

8.8. INFORMACIÓN SOBRE UNA POSIBLE CESIÓN DE DATOS

La persona donante de sus datos debe permitir o no el traspaso de sus datos a un tercero **antes** de compartir, comunicar, o dejar que otro acceda a ellos.

Ten en cuenta que la comunicación de datos a un Encargado del tratamiento, con el que tienes firmado un contrato o convenio, no se considera una cesión de datos, ya que dicho Encargado sólo tratará los datos conforme a las instrucciones que tú le des, y se haya firmado el respectivo Acuerdo o *Contrato de tratamiento de datos* o más conocido como Acuerdo de Confidencialidad entre Responsable y Encargado.

Se ampliará la información sobre la cesión de datos en el Apartado 10 de esta Guía.

> *Ten en cuenta …*
>
> *Si has firmado un contrato o un convenio con quien será el Encargado del tratamiento de los datos personales, recuerda que también hay que suscribir (con el Encargado) un "Contrato de tratamiento de datos" o también llamado "Acuerdo de confidencialidad".*

8.9. INFORMACIÓN SOBRE LA POSIBLE TRANSFERENCIA INTERNACIONAL DE DATOS

Se entiende por transferencia internacional de datos cuando los datos personales se van a ceder fuera del territorio del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega) o a países que no garantizan un nivel de protección adecuado según indica la Comisión Europea. Como en el caso anterior, la persona donante de sus datos personales debe permitir o no el traspaso internacional de sus datos, y se le debe informar de ello.

En la siguiente URL de la Agencia Española de Protección de Datos (AEPD) se muestra una lista de los países que han sido considerados por la Comisión Europea que garantizan un nivel de protección adecuado: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-

cumplimiento/transferencias-internacionales. Este listado puede verse ampliado o disminuido con el transcurso del tiempo, por lo que se aconseja revisarlo antes de realizar dicho tratamiento.

Se ampliará la información sobre la transferencia internacional de datos en el Apartado 11 de esta Guía.

VOLVER AL INICIO DEL DOCUMENTO

9. RECABAR EL CONSENTIMIENTO

El consentimiento de la persona donante de sus datos personales es la expresión libre de que acepta que trates su información -sus datos- para una finalidad concreta, bajo unas determinadas condiciones de las cuales ha sido previamente informada.

Actualmente todavía existen prácticas que se encuadraban en el llamado *consentimiento tácito*, pero debes saber que han dejado de ser aceptables: el silencio, la inacción o las casillas previamente seleccionadas como forma de recabar el consentimiento, como supuesta aceptación de la donación de datos, **ya no son válidas**.

> *Ten en cuenta que …*
>
> *El consentimiento, previamente informado, debe ser expreso. Debe aceptar expresamente el tratamiento de sus datos, en los términos en que se ha informado. No es válido el denominado "consentimiento tácito".*

9.1. LAS CARACTERÍSTICAS DEL CONSENTIMIENTO

El consentimiento debe ser:

- *Explícito*: la persona donante o participante en tu investigación emite una declaración de consentimiento expresa (siempre una clara acción afirmativa). Por ejemplo, la firma de un documento o pulsar la acción "Acepto" o marcar el check adecuado en un entorno electrónico.
- *Libre*: prestado en un marco de libertad, no puede estar condicionado a, por ejemplo, una rebaja en una tarea académica, la consecución de un bien material, o a cualquier otro tipo de condición. Al evaluar si el consentimiento se ha dado libremente, siempre has de tener en cuenta la posible existencia de condiciones que limiten esa libertad de decisión.
- *Informado*: para que el consentimiento sea realmente informado, la persona posible donante debe saber y entender qué está decidiendo y, para ello, se lo has de explicar de manera comprensible.
- *Inequívoco*: la información que ofrezcas a las personas participantes en tu investigación sobre la prestación de su consentimiento para donarte sus datos debe estar muy clara y no mezclada con otras condiciones de la investigación o con otras solicitudes para donación de muestras, la realización de encuestas,

etc. (Ver "Deber de informar - ¿Cuál será el contenido de la información aportada?").

- *Específico*: tienes que recabar el consentimiento para cada finalidad y explicar bien que no vas a usarlos para otros fines.
- *Verificable*: como responsable del tratamiento específico debes poder demostrar ante cualquier autoridad competente, persona o comité pertinente, que la persona donante te consintió el tratamiento de sus datos personales para los fines de tu investigación.(Ver "Deber de informar - Custodia").
- *Distinguible y manifiesto*: si el consentimiento para la recogida, uso y conservación de sus datos te lo da la persona donante en el texto y en el contexto del consentimiento para participar en tu proyecto de investigación, tienes que presentársela de manera que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso, y utilizando un lenguaje claro y sencillo.
- *Revocable*: las personas participantes en tu investigación pueden retirar el consentimiento en cualquier momento, y has de informarle de que puede solicitarlo de manera sencilla y que dicha revocación no tendrá consecuencias para ella y, además, debes indicarle cómo hacerlo. Además, la revocación no surtirá efectos retroactivos, sino que los datos personales de dichas personas no se tratarán a partir de ese momento en tu investigación.

> *Recuerda que …*
>
> *El consentimiento debe ser explícito, libre, informado, inequívoco, específico, verificable, distinguible y manifiesto, así como revocable.*

9.2. VALIDEZ DEL CONSENTIMIENTO RECABADO ANTES DE LA ENTRADA EN VIGOR DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

Si para realizar tu proyecto de investigación, obtuviste el consentimiento **antes** de mayo de 2018 **no** tienes obligación de recabar de nuevo el consentimiento con las condiciones del RGPD, ya que cuando te lo dieron esa norma no era todavía aplicable. Pero, por diligencia y honradez se recomienda facilitar la nueva información a las personas participantes en tu proyecto, en la medida de lo posible.

9.3. CONSENTIMIENTO RECABADO DE FORMA ELECTRÓNICA

El consentimiento informado recabado de forma electrónica es tan válido como el recogido en papel, y si no quieres tener documentación en papel y prefieres tener todo en formato electrónico, incluso puedes recogerlo con firma digital o con certificado electrónico, aunque esta posibilidad todavía sea difícil de utilizar por todas las personas participantes. Recuerda que en todos los casos la persona donante debe realizar una clara acción afirmativa para que pueda considerarse válido su consentimiento y que has de mantener esos consentimientos, con los datos de los donantes, también protegidos.

La aceptación mediante un clic en una casilla, en que dejes expresamente la posibilidad de decidir si acepta o no el tratamiento de los datos, se considera un consentimiento válido siempre que **NO** lo hagas a través de **casillas premarcadas**.

9.4. CONSENTIMIENTO PRESTADO CUANDO TRABAJES CON DATOS ESPECIALMENTE PROTEGIDOS

Para tratar datos sensibles o especialmente protegidos en tu investigación, como pueden ser los datos de salud, por ejemplo, necesitas el consentimiento de las personas participantes en tu investigación, salvo que te los seudonimice una persona que sea ajena técnica y funcionalmente de tu equipo investigador. Es decir, que no es garantía suficiente que la seudonimización la hagáis tú o alguien de tu equipo investigador cuando no se cuenta con el consentimiento de la persona donante.

Las exigencias al respecto de los datos sensibles o especialmente protegidos en investigación son exigibles no sólo en el área de salud sino también en otras áreas de investigación en tanto en cuanto se trata de datos de carácter especial (ciencias biológicas, biomédicas, sociales, jurídicas y de la conducta). La regulación actual, tras la aprobación del RGPD en 2016 y la LOPDGDD de 2018, es **más exigente** con el consentimiento expreso, ya que antes se aceptaba en algún caso –en situaciones de transacciones comerciales, especialmente- el consentimiento tácito, pero nunca para supuestos de investigación.

Recuerda que …

La normativa vigente refuerza la necesidad del consentimiento como regla general, si bien ofrece, en caso de la investigación en salud y biomédica, la posibilidad de utilizar los datos seudonimizados por personas ajenas a la investigación.

(Ver "¿Qué es un dato personal? – Datos de salud" y en la Sección sobre SALUD de la AEPD, en el epígrafe "Investigación sanitaria y ensayos clínicos").

9.5. CONSENTIMIENTO PRESTADO POR MENORES DE EDAD

El tratamiento de los datos personales de un menor -recogida, uso y conservación- requiere su consentimiento. El consentimiento prestado por mayores de 14 años se presupone válido y para los menores de 14 años es necesario que también autoricen sus progenitores o tutores. Recuerda que, si vas a recabar datos *on line* de menores tienes que establecer procedimientos para que se pueda verificar el consentimiento parental.

(Ver "¿Qué es un dato personal? – Datos de menores").

9.6. CUSTODIA DE CONSENTIMIENTOS

Como persona investigadora responsable debes tener guardados, en formato electrónico o en papel, todos los consentimientos de las personas donantes, para el tratamiento de sus datos. Estos documentos te van a permitir, en caso necesario, demostrar la legitimidad para la realización de dicho tratamiento. Tanto en formato papel o electrónicamente, debes guardarlos de manera segura en una ubicación que ofrezca todas las garantías de seguridad.

Desde la Unidad de Protección de Datos de la UAH se aconseja la **utilización del servicio One Drive** como un lugar para almacenar la información en formato electrónico de tu investigación, al ser un servicio validado por la UAH en cuanto a la seguridad de la información se refiere, y que cumple con las máximas garantías en este sentido. Por este motivo, nos parece una buena idea que la información a tratar, incluidas las entrevistas o grabaciones de voz y/o imagen, se encuentre en One Drive. Todos los miembros de la Comunidad universitaria de la UAH tienen a su disposición un espacio disponible en One Drive.

La utilización de ordenadores personales fuera del dominio de la UAH -como probablemente será el ordenador de tu propiedad-, así como los discos duros/USB que se utilicen durante la investigación, deben estar cifrados para ofrecer una mayor seguridad de la información que contienen.

Por otro lado, la información de tu investigación que se encuentre en **formato papel**, debe ser guardada en sitios - cajones/armarios- que ofrezcan una seguridad de la información adecuada, como el uso de una llave física o lógica de acceso a la misma.

RESUMEN "RECABAR EL CONSENTIMIENTO"

Antes de solicitar sus datos personales a las personas participantes de la investigación se les debe informar detalladamente en qué consiste la actividad o proyecto de investigación que vas a llevar a cabo, y también se tiene que solicitar a los participantes su consentimiento expreso e informado, y tienen que firmarlo. Su participación siempre será de forma voluntaria.

Por tanto, en cuanto a los **consentimientos expresos e informados** hay que tener en cuenta que éstos deberán explicar de forma clara y sencilla cuál es el objeto de la investigación, pero especificando, si fuera el caso, también, si se va a difundir-publicar, si va a existir una cesión de datos personales a otra entidad o si se van a realizar transferencias internacionales, por ejemplo. Pero no de una forma vaga sino especificando claramente quién y cómo se van a tratar sus datos y para qué. Debe quedar claro que no pueden utilizarse los datos para otra finalidad distinta a la especificada y tampoco habrá cesiones o transferencias internacionales de datos personales a entidades distintas a las especificadas en dicho consentimiento. Estos consentimientos deberán ser firmados por las personas que van a participar en el estudio o actividad de investigación.

Además, los documentos con la información y los consentimientos expresos firmados por las personas participantes, se tienen que guardar para tener constancia de las acciones llevadas a cabo, y poder demostrar que se han hecho, por si fuera necesario mostrarlo ante la Autoridad de Control competente (AEPD y Autoridades autonómicas). Además, se debe dar una copia a las personas participantes de todo lo que firmen, incluida la información facilitada sobre el tratamiento a llevar a cabo, y tener en cuenta que dichas personas participantes pueden revocar dicho consentimiento cuando lo deseen, y en tal caso, se deberán de dejar de tratar sus datos a partir de ese momento.

VOLVER AL INICIO DEL DOCUMENTO

10.CESIÓN O COMUNICACIÓN DE DATOS

Si tienes que ceder datos de carácter personal a terceros ajenos a la investigación (los terceros son aquellos que NO son ni las personas interesadas, ni las personas investigadoras autorizadas, ni las personas encargadas de tratamiento) es obligatorio que obtengas el consentimiento expreso y escrito de la persona que te los donó.

Hay una situación especial que debes considerar: si la información que vas a comunicar a terceras personas incluye datos obtenidos de la persona participante en tu investigación, que revelan o pueden revelar información *de carácter personal de sus **familiares***, la cesión requerirá también el consentimiento expreso y escrito de todos ellos.

Ten en cuenta que …

Si tienes que ceder datos de carácter personal a terceros ajenos a la investigación es obligatorio que obtengas el consentimiento expreso y escrito de la persona que te los donó. Y, si fuese el caso, habrá que conseguir idéntico consentimiento de sus familiares, si de la información obtenida se revela o se puede revelar información personal de aquellas personas.

VOLVER AL INICIO DEL DOCUMENTO

11.TRANSFERENCIAS INTERNACIONALES

Debes tener especial cuidado, en cuanto a la protección de datos se refiere, si en tu proyecto de investigación vas a colaborar con otros grupos de investigación que están fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

Las transferencias internacionales de datos suponen un flujo de datos de carácter personal desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo. Tanto tú, como investigador/a, como la institución en la que investigas, que es responsable del tratamiento, seréis exportadores porque estáis en territorio europeo y vais a realizar esa transferencia internacional.

> *Recuerda que…*
>
> *Hay que prestar mucha atención al hecho de que la investigación pueda suponer, en cuanto a datos personales se refiere, que vamos a realizar una transferencia internacional. Si desde la UAH colaboras con otras personas integradas en Proyectos o Grupos que están fuera del Espacio Schengen, ¡ten especial cautela!*

Sólo puedes realizar transferencias de los datos personales de la investigación a un país u organización internacional si garantizan un nivel de protección adecuado de acuerdo con las condiciones establecidas en el Capítulo V del RGPD. Cuando los datos vayan a ser transferidos **fuera** del Espacio Económico Europeo a algún país, territorio o sector específico de ese tercer país u organización internacional que la Comisión Europea no haya considerado que garanticen un nivel de protección adecuado, debe darse alguna o algunas de las circunstancias recogidas en el mencionado Capítulo —cuya extensión casuística excede las pretensiones de esta Guía— que autoricen dicha transferencia.

En la siguiente URL de la AEPD se muestra una lista de los países que han sido considerados por la Comisión Europea como garantes de un nivel de protección adecuado: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales. Este listado puede verse ampliado o disminuido con el transcurso del tiempo, por lo que se aconseja revisarlo antes de realizar dicho tratamiento.

Por otro lado, si los datos personales de la investigación vas a albergarlos en la "nube" (*Cloud Computing*) es importante que tengas en cuenta que muchas de las empresas que prestan dichos servicios están ubicadas fuera del referido Espacio Económico Europeo y no proporcionan las garantías jurídicas adecuadas. Si utilizas la "nube" OneDrive de Microsoft no tendrás problemas, en cuanto a la protección de datos se refiere, ya que la UAH tiene firmado con dicha empresa un Contrato de tratamiento de datos o Acuerdo de Confidencialidad que ampara dicho alojamiento.

VOLVER AL INICIO DEL DOCUMENTO

12.CONSERVACIÓN DE LOS DATOS Y PREVISIÓN DE SU DESTRUCCIÓN

En cuanto al **tiempo que se tiene que almacenar o custodiar la documentación** generada en el Proyecto de Investigación, ya sea un TFG, TFM, Tesis Doctoral o Proyecto, tanto el RGPD como la LOPDGDD no indican un plazo de conservación determinado, sino que establecen que este plazo será el estrictamente necesario para cumplir con la finalidad para la que los datos personales fueron recogidos (Principio de conservación).

La legislación, como ya se ha dicho, indica que los datos podrán conservarse durante periodos *más largos* siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos -por lo que también podrían conservarse durante más tiempo (sin especificar en la legislación, tampoco un plazo concreto) por tratarse de una investigación científica-, y podrían destruirse los datos cuando finalice el proceso de edición, garantizando durante ese plazo las adecuadas medidas de custodia de los datos.

Como se ha comentado, desde la Unidad de Protección de Datos se aconseja **la utilización del servicio One Drive** como el lugar más conveniente para almacenar la información de tu TFG, TFM, Tesis Doctoral o Proyecto de Investigación, al ser un servicio validado por la UAH en cuanto a la seguridad de la información se refiere, cumpliendo con las máximas garantías en este sentido. Por este motivo, nos parece una buena idea que toda la información a tratar se encuentre en One Drive, incluyendo entrevistas de audio y vídeo, encuestas, o cualquier otro dato personal que trates. Todos los miembros de la Comunidad universitaria de la UAH tienen a su disposición un espacio disponible en One Drive.

La utilización de ordenadores personales fuera del dominio de la UAH -como probablemente será el ordenador de tu propiedad-, así como los discos duros/USB que se pudieran utilizar, deben estar cifrados para ofrecer una mayor seguridad de la información que contienen.

Por otro lado, veíamos que la información de tu TFG, TFM, Tesis Doctoral o Proyecto de Investigación que se encuentre en **formato papel**, debe ser guardada en sitios -cajones/armarios- que ofrezcan una seguridad de la información adecuada, como el uso de una llave física o lógica de acceso a la misma.

Desde esta Unidad también se recomienda que se realicen copias de seguridad periódicamente de la información tratada, y mantener a salvo los datos tratados.

En cuanto a la **Eliminación de los datos personales** recogidos en su trabajo de investigación, ésta eliminación dependerá de si se encuentran en soporte papel y/o soportes digitales. Si estos documentos estuvieran en papel se llevará a cabo una destrucción física mediante el uso de una destructora de papel ya sea personal o utilizando los medios que ofrece la UAH a través de una empresa especializada contratada a tal efecto. Si los datos personales de los documentos están en soportes digitales, la eliminación se llevará a cabo dependiendo del tipo de soporte en el que se encuentre la información. Para el caso de los soportes electrónicos (pen-drive o Lápiz de memoria) la destrucción de la información puede llevarse a cabo mediante los procesos de destrucción física o sobrescritura. Para el caso de los soportes magnéticos (discos duros) la destrucción de la información puede llevarse a cabo mediante los procesos de desmagnetización, destrucción física o sobrescritura. Cuando queremos reutilizar los soportes magnéticos y electrónicos podremos utilizar el formateo a bajo nivel para asegurarnos de que se imposibilita la recuperación de la información en todo el soporte.

Como ya se ha dicho en otros apartados, e insistimos aquí, los datos personales que se soliciten de las personas participantes en su investigación deben ser los estrictamente necesarios para la finalidad de la gestión que se va a llevar a cabo, ya que se debe cumplir el Principio de Minimización de los datos que indica que los datos deben ser *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"* (Art. 5.1.c) RGPD).

VOLVER AL INICIO DEL DOCUMENTO

13.PUBLICACIÓN DE LOS RESULTADOS DE LA INVESTIGACIÓN

En cuanto a la publicación de los resultados de su actividad de investigación, ya sea un TFG, TFM, Tesis Doctoral o Proyecto de investigación, bastaría con indicar que la publicación de los resultados se hará en revistas especializadas, en un libro, capítulo de un libro, etc. No es necesario especificar el nombre de dónde se hará dicha publicación (editorial u *Open Access*) ya que, en un inicio, todavía no sabréis si dicha publicación va a realizarse y dónde.

Por otro lado, los datos publicados serán los **resultados de su investigación, no los datos personales** de las personas participantes en ella, y tampoco los datos personales utilizados para la investigación que, además, podría tratar datos de los llamados especialmente protegidos, y hay que cuidar este extremo, por ejemplo, **anonimizando los datos**.

> *Encontrarás información útil de cómo anonimizar los datos personales en el apartado de la Agencia Española de Protección de Datos (AEPD) llamado "Guía y Herramienta básica de anonimización"*

VOLVER AL INICIO DEL DOCUMENTO

14.ANÁLISIS DE RIESGOS

> *"El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten".* Agencia Española de Protección de Datos (AEPD)

Como señala la AEPD tienes que analizar la naturaleza de tu investigación, el contexto en el que se desarrolla y su finalidad, para saber los posibles riesgos de que un *impacto negativo*, sobre los datos personales que tratas, afecte a los derechos y libertades de las personas que te los han suministrado. Las dimensiones de seguridad de la información que has recogido y que pueden verse afectadas por un incidente o brecha son:

1. *Confidencialidad*: propiedad de la información de no ser revelada a personas no autorizadas. Posible incidente: *revelación, robo…*
2. *Integridad*: propiedad de la información de no ser alterada sin autorización y conservar su exactitud. Posible incidente: *alteración, manipulación…*
3. *Disponibilidad*: propiedad de la información de estar accesible para las personas autorizadas. Posible incidente*: inaccesibilidad, pérdida…*
4. *Trazabilidad*: propiedad de la información que identifica de una manera unívoca a las personas o procesos que acceden a la información y las acciones que han realizado.
5. *Autenticidad*: propiedad de la información que garantiza que una entidad es quien dice ser o bien que se garantiza la fuente de la que proceden los datos.

El análisis de riesgos (AR) consiste en analizar las probabilidades de que, en un momento dado, pueda verse afectada alguna de las cinco dimensiones o propiedades de la información. Hay que plantearse la hipótesis de que personas no autorizadas accedan a los datos de tu investigación, que los datos sean manipulados indebidamente de forma accidental o deliberada, que no puedas acceder a los datos de la investigación por un incidente o que deje de identificarse a las personas que acceden a la información y qué acciones han realizado.

Tras imaginar esas posibilidades reales (riesgo bajo/riesgo alto), tienes que valorar qué daño (leve/grave) puede causar a los derechos de las personas donantes si éstos se producen, y establecer unas medidas de seguridad (sencillas/complejas) en función del nivel y del tipo de riesgo.

Es importante que los equipos de investigación tengáis claro que:

1. Debéis realizar el análisis de escenarios concretos de posibles amenazas para la seguridad de los datos personales manejados en vuestra investigación. Por ejemplo, en el caso de un consentimiento informado en papel que siempre contiene la firma de los participantes, su pérdida o uso ilegítimo puede facilitar la suplantación de su identidad en documentos legales de todo tipo. Otra fuente de incidentes es el envío de información con datos personales sin cifrar a otros miembros del equipo investigador, y que puedan ser interceptados por terceros no autorizados.
2. Es recomendable la utilización del equipamiento informático corporativo de la UAH que es el que incorpora medidas de seguridad "por defecto". Si esto no fuera posible, el equipamiento utilizado debe incorporar medidas de seguridad equivalentes al equipo suministrado por la Universidad.

Como ya se ha comentado, hay que tener en cuenta que una *brecha de seguridad* es un incidente de seguridad que afecta a datos de carácter personal.

14.1. PUBLICACIONES EN LA AGENCIA DE PROTECCIÓN DE DATOS (AEPD)

Para evaluar los riesgos que un tratamiento de datos personales representa para los derechos y libertades de las personas interesadas cuyos datos son tratados es preciso llevar a cabo, en primer lugar, la identificación de dichos riesgos para, posteriormente, gestionarlos a lo largo de todo el ciclo de vida del tratamiento, es decir, desde su diseño hasta que la actividad de tratamiento deje de ser necesaria.

Ten en cuenta que …

Para evaluar los riesgos de un tratamiento de datos personales es preciso identificar dichos "riesgos" y, después, gestionar su tratamiento desde su diseño inicial hasta que finalice.

Con el objetivo de ayudar en el análisis de riesgos orientado a determinar las medidas de seguridad, la AEPD ofrece indicaciones en la Guía Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.

Del mismo modo, la AEPD ha puesto a disposición la herramienta FACILITA-RGPD a utilizar cuando se realice un tratamiento de datos personales de *escaso riesgo* para el cumplimiento del Reglamento General de Protección de Datos. No podrá utilizarse para tratamientos que impliquen un alto riesgo para los derechos y libertades de las personas, como datos de salud o tratamientos masivos de datos, entre otros.

VOLVER AL INICIO DEL DOCUMENTO

15.EVALUACIÓN DE IMPACTO

El RGPD indica que *"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales"*.

Si después de la realización del Análisis de Riesgos (AR) concluyes que el tratamiento de datos que se necesita para la investigación conlleva un *riesgo significativo o alto* para los derechos de las personas participantes, tendrás que realizar una *Evaluación de Impacto (EIPD)*. Es decir, un proceso sistemático con una metodología determinada para analizar los riesgos significativos que tu investigación puede comportar para la protección de los datos, o los derechos y libertades de las personas que te los han donado.

> El RGPD no obliga a que para cualquier tratamiento de datos personales sea necesario realizar una EIPD, pero sí establece que es obligatorio que se realice cuando hay una probabilidad de que entrañe un alto riesgo. Por tanto, la existencia de un grado razonable de potencial *alto riesgo* hace imprescindible la realización de una EIPD.

De tal forma que la EIPD es una herramienta para situaciones de alto riesgo o para cuando utilizas grandes cantidades de datos especialmente protegidos (art. 35 RGPD).

El objetivo de la EIPD es determinar:

a) la *probabilidad* de que se produzcan situaciones no deseadas
b) la *gravedad* de sus consecuencias y
c) las *medidas de contención* que tenemos que tomar para evitar o paliar sus consecuencias

De esta forma, puedes establecer el *Nivel de Riesgo Inicial* de las operaciones de recogida y uso de datos que has diseñado para llevar a cabo tu proyecto de investigación y el *Nivel de Riesgo Residual Aceptable* una vez llevadas a cabo las medidas de contención o seguridad.

Gracias a esta EIPD puedes concretar y describir las *medidas de seguridad o contención*

y los protocolos adecuados que has previsto inicialmente para reducir, prevenir y corregir los riesgos (probabilidad y gravedad) en cada momento clave de la recogida, el uso y la conservación de los datos necesarios para tu investigación.

15.1. RECOMENDACIÓN U OBLIGACIÓN DE LA EIPD

Recuerda que la EIPD no siempre es necesaria, pero es recomendable que, al plantearte cada nueva recogida y uso de datos, hagas un Análisis de riesgos (AR) para determinar la conveniencia o no de realizar una EIPD.

¿Cuándo la EIPD es **OBLIGATORIA**? ¿Para qué tipología de investigaciones?

1. *De alto riesgo*: la recogida, uso y guarda de sus datos pueden entrañar un alto riesgo para los derechos y libertades de las personas físicas. Ej. personas emigradas por razones de ideología o identidad sexual.
2. *Evaluación sistemática*: cuando, sistemáticamente, se recojan y evalúen aspectos personales de personas físicas basadas en un tratamiento automatizado. Ej. elaboración de perfiles.
3. *Uso de tecnologías invasivas de la privacidad:* en el proyecto de investigación se utilizarán: aeronaves no tripuladas (drones); minería de datos; biometría; técnicas genéticas; geolocalización; videovigilancia a gran escala; vigilancia electrónica.
4. *Tratamiento a gran escala de datos especialmente protegidos*, que serían por ejemplo investigaciones:
    - Que requieren de una gran cantidad de datos (volumen, variedad y duración o permanencia de la actividad de recogida, uso y guarda de datos).
    - En un ámbito geográfico regional o superior (zonas geográficas amplias, gran extensión geográfica de la actividad de recogida, uso y guarda de datos).
    - Que afectan a gran número de personas (bien en términos absolutos, bien como proporción de una determinada población).
    - Referidas a datos sensibles como biométricos, de salud, etc. y también que incluyan datos personales relativos a menores y a personas vulnerables.
    - En las que se aplican nuevas tecnologías (que puedan tener riesgos para la privacidad) a esa gran escala.

- Que entrañan alto riesgo para los derechos y libertades de las personas interesadas.

15.2. CONTENIDOS DE LA EIPD

El resultado final de la EIPD tiene que ser un *Informe de evaluación de impacto o* un *conjunto de documentación* que informe adecuadamente y recoja las características del tratamiento evaluado y de la gestión de los riesgos, es decir, de las decisiones tomadas para mitigarlos. Este informe, cuando lo haya, quedará recogido con el resto de la documentación en tu archivo de documentación sobre protección de datos de tu investigación concreta.

Ese INFORME DE EVALUACIÓN DE IMPACTO **tiene que incluir**:

1. *Análisis del proyecto*: donde nuevamente se detallan las *categorías* de datos que recogerás, usarás y guardarás, las *personas* que podrán acceder a ellos, los *flujos* de información y las *tecnologías* utilizadas.
2. *Juicio de proporcionalidad*: en el que se discierne/dirime si la finalidad que persigues se puede conseguir por otros medios, por ejemplo, usando otros datos o menos datos, reduciendo el colectivo de personas donantes cuantitativa o cualitativamente, con otras tecnologías menos invasivas o aplicando otros procedimientos o medios de tratamiento, etc. Este juicio se asienta en tres aspectos a revisar que ya has trabajado en la primera fase:
   a) Idoneidad: los datos recogidos sirven para conseguir el objetivo propuesto con la investigación.
   b) Necesidad: no existe otra forma más moderada para llevar a cabo la investigación con la misma eficacia.
   c) Proporcionalidad: es ponderada o equilibrada, porque se derivan más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.
3. *Evaluación de los riesgos*: apartado donde analizas los posibles riesgos para la protección de datos de las personas afectadas, que ya has confirmado en los puntos anteriores que necesitarás y valoras su probabilidad y el impacto de su materialización.
4. *Medidas previstas:* incluyes las medidas que vas a establecer para afrontarlos.

Recuerda que…

Tras la EIPD hay que elaborar un Informe de evaluación de impacto o conjunto de documentación que acredite convenientemente las características del tratamiento evaluado y de la gestión de los riesgos: ¿qué decisiones tomarás para mitigar los riesgos? El Informe incluirá análisis del proyecto, juicio de proporcionalidad (idoneidad, necesidad y ponderación equilibrada), evaluación de los riesgos, y medidas previstas.

Ten en cuenta que la obligatoriedad de hacer la EIPD es consecuencia de la naturaleza, la metodología y los medios utilizados en la investigación. Por tanto, es bueno replantear aspectos éticos y metodológicos que permitan abordar la investigación con un menor nivel de impacto en la privacidad y los derechos de las personas participantes. Muchas veces no es posible, y es entonces cuando hay que replantearse sinceramente la pertinencia de la metodología pensada para la investigación frente al riesgo que supone para la privacidad y derechos de las personas donantes. Si la respuesta es afirmativa, su justificación constituye la EIPD y debe ser lo más razonada y minuciosa posible, en los términos anteriormente explicados.

15.3. PUBLICACIONES EN LA AGENCIA DE PROTECCIÓN DE DATOS (AEPD)

En junio del 2023, la Agencia Española de Protección de Datos (AEPD) ha lanzado una nueva versión de su herramienta GESTIONA RGPD, orientada especialmente a pequeñas entidades públicas o privadas –que te puede servir de orientación en tu investigación-, y que permite gestionar los tratamientos, realizar la gestión de riesgos y, en su caso, dar soporte para la realización de las evaluaciones de impacto. “Gestiona RGPD” (AEPD) se ha rediseñado con un formato más intuitivo e incorpora las últimas directrices recogidas en las guías publicadas por la Agencia.

Además, en septiembre de 2023, la AEPD ha elaborado una nueva versión de la guía que contiene las “Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo”

La AEPD también ha elaborado dos listados de aquellos tratamientos en los que:

- **NO** es necesario realizar una Evaluación de Impacto relativa a la Protección de datos https://www.aepd.es/sites/default/files/2019-12/ListasDPIA-35.5l.pdf
- **SI** es necesario realizar una Evaluación de Impacto relativa a la Protección de datos https://www.aepd.es/documento/listas-dpia-es-35-4.pdf

VOLVER AL INICIO DEL DOCUMENTO

16.GARANTIZAR LA SEGURIDAD

El Artículo 5.1.f del RGPD determina la necesidad de que establezcas garantías de seguridad adecuadas que eviten, fundamentalmente:

- El tratamiento no autorizado o ilícito de los datos personales que has solicitado.
- La pérdida de esos datos personales, su destrucción o el daño accidental.
- La falta de disponibilidad de los datos.

Para que no ocurra, tienes que establecer unas medidas técnicas y organizativas que aseguren la integridad, la confidencialidad y la disponibilidad pero que, además, te permitan demostrar (cuando se requiera en supervisión o auditoría o solicitud de la Autoridad de Control competente) que las estás llevando a la práctica durante y después de la investigación.

Porque, como se ha dicho, el RGPD nos indica que *"[…] el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo"*. Y para conseguir el nivel de seguridad adecuado, la LOPDGDD nos dice que "*El Esquema Nacional de Seguridad incluirá las medidas de seguridad que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679"* [Disposición Adicional Primera de LOPDGDD].

> *El vigente ENS -que ha experimentado una evolución continua desde su primer desarrollo en 2010-, establece la política de seguridad para la protección adecuada de la información tratada y los servicios prestados a través de un planteamiento común de principios básicos, requisitos mínimos, medidas de protección y mecanismos de conformidad y monitorización, tanto para la Administración Pública, como para los proveedores tecnológicos del sector privado que colaboran con la administración. El ENS tiene por finalidad la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las Comunicaciones, y los servicios electrónicos, que permitan a la ciudadanía y a las Administraciones Públicas el ejercicio de los derechos y el cumplimiento de los deberes a través de estos medios.*

A continuación, se indican algunas de las Medidas de seguridad técnicas y organizativas a tener en cuenta en tu investigación. No obstante, dependiendo de los datos personales tratados estas medidas de seguridad se ampliarán siguiendo el mencionado Esquema de Seguridad (ENS).

16.1. MEDIDAS DE SEGURIDAD ORGANIZATIVAS

Todas las personas de tu equipo de investigación han de saber que tienen un deber de confidencialidad que persiste cuando finalice la investigación, y también que deben evitar el acceso de personas no autorizadas a tratar los datos. Es conveniente que todas aquellas personas que vayan a tener acceso a los datos, firmen un documento de confidencialidad.

> *Todos los grupos de investigación van a tener que formarse y entrenarse en esta parte de las tareas para llevar adelante sus Proyectos. Es importante que se plantee todo esto dentro del propio diseño de la investigación ya que requiere tiempo, trabajo, así como recursos humanos y materiales.*

Para hacer efectivos esos deberes al diseñar del proyecto debes implantar las siguientes medidas organizativas:

1. Es conveniente adoptar unas Normas de seguridad para el tratamiento de los datos conocida por todo tu equipo investigador. En nuestro caso, dichas normas deben ser compatibles con la Política de Seguridad de la Información de la Universidad de Alcalá [Aprobada por el Consejo de Gobierno de la UAH, el 15 de julio de 2020].
2. Distribución de *Roles y responsabilidades*. Hay que designar específicamente quién va a ser la persona responsable de la seguridad dentro de tu equipo investigador.
3. Organizar la gestión de los ordenadores, del software, de los dispositivos de almacenamiento y de los recursos de red.
4. Formación en *medidas de seguridad cotidianas y el cumplimiento de las mismas:*
    - No dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.).
    - Proceder antes de ausentarse al bloqueo de la pantalla o al cierre de la sesión; almacenar los documentos en papel y soportes electrónicos en lugar seguro

(armarios o estancias de acceso restringido) durante las 24 horas del día.

- No comunicar datos o cualquier información personal a terceros, especialmente durante las consultas telefónicas, correos electrónicos, etc.

5. Establecer *Procedimientos seguros de acceso y respuesta* a la persona que ha donado sus datos cuando quiera ejercer sus derechos: medios electrónicos, remisión a la persona Delegada de Protección de datos (DPD), a la dirección postal de Universidad, etc.
6. Seguir el *Protocolo de actuación establecido ante una violación de la seguridad*: en caso de acceso indebido a los datos personales, una alteración de la información o una pérdida del acceso, debes ponerte en contacto de inmediato con tu DPD para registrar el incidente y evaluar sus consecuencias. Si la brecha de seguridad puede constituir un riesgo para los derechos y libertades de las personas físicas que participan en tu investigación tienes que informarles a ellas sin dilación indebida y a la institución (UAH, en nuestro caso) a través del DPD, y notificarlo a la Agencia Española de Protección de Datos en un máximo de 72 horas, incluyendo toda la información necesaria para esclarecer los hechos.

16.2. MEDIDAS DE SEGURIDAD TÉCNICAS

Las medidas técnicas son decisiones de seguridad elementales para evitar riesgos o minimizarlos que tienen que ser revisadas periódicamente de manera automática (software o programas informáticos) o manual:

1. *Control de acceso y autentificación: perfiles y contraseñas:*
   a) Dispón de varios perfiles o usuarios distintos para cada finalidad: cuando utilicéis el mismo ordenador o dispositivo para el tratamiento de datos personales de la investigación y para otros fines de uso personal o profesional, se recomienda mantener separados dichos usos.
   b) Dispón de perfiles con derechos de administración para la instalación y configuración del sistema y perfiles de usuarios sin privilegios o derechos de administración para el acceso a los datos personales: esta medida evita que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
   c) Garantiza la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos, con al menos 12 caracteres, mezcla de números, letras (mayúsculas y minúsculas) y caracteres especiales. Léase la Política de Contraseñas de la Universidad de Alcalá [Aprobada por el Comité de Seguridad de la Información y Seguridad TIC de la UAH en su sesión de 15 de marzo de 2024].

d) Identificación inequívoca: cuando vayan a acceder distintas personas a los datos, dispón para cada una de un usuario y contraseña específicos.

e) Contraseñas: debes garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso pueden compartir las contraseñas ni dejarlas anotadas en lugar común ni acceso a personas distintas de la usuaria.

2. *Archivo de registro de accesos: actividad, monitorización y seguimiento:*

   El uso de archivos de registro de accesos es una medida de seguridad importante que permite la identificación y el seguimiento de las acciones con los datos personales.

3. *Seguridad de los puestos de trabajo, servidores y redes:*

   a) Actualización: tienes que asegurarte de mantener la actualización de ordenadores y dispositivos en la media posible.

   b) Antivirus: en los ordenadores y dispositivos donde realices el tratamiento automatizado de los datos personales dispón de un sistema de antivirus, actualizándolo de forma periódica.

   c) Cifrado: la seguridad de la red es importante tanto respecto a las conexiones externas (por ejemplo, a Internet), como a la interconexión con otros sistemas (externos o internos) de la propia universidad. Cuando realices el acceso a través de Internet, cifra la información con protocolos criptográficos (TLS/SSL).

   d) Cortafuegos y detección de intrusos: monitoriza el tráfico hacia y desde el sistema de información con Cortafuegos y Sistemas de Detección de Intrusos.

   e) Segregación: la red de datos debe segregarse de lasotras redes.

4. *Cifrado de datos:*

   Cuando precises mover datos personales, ya sea por medios físicos o por medios electrónicos, utiliza un método solvente de cifrado.

5. *Copias de seguridad:*

   Periódicamente realiza una copia de seguridad en un segundo soporte distinto del que utilizas para el trabajo diario. Almacena la copia en un lugar seguro, distinto de aquél en el que tengas ubicado el ordenador con los ficheros originales, así podrás recuperar los datos personales en caso de pérdida de la información.

6. *Destrucción adecuada de dispositivos y eliminación de datos:*

   La UAH pone a disposición de la Comunidad universitaria la posibilidad de realizar una destrucción segura de dispositivos y de papel, ya que tiene contratada una empresa que realiza estas funciones y con la que la Universidad tiene firmado un Acuerdo o Compromiso de Confidencialidad.

7. *Seguridad física de las instalaciones.*

7 MEDIDAS TÉCNICAS DE SEGURIDAD

DURANTE LA INVESTIGACIÓN

1. *Control de acceso y autentificación: perfiles y contraseñas*
2. *Archivo de registro de accesos: actividad, monitorización y seguimiento*
3. *Seguridad de los puestos de trabajo, servidores y redes:*
   - *Actualización*
   - *Antivirus*
   - *Cifrado*
   - *Cortafuegos y detección de intrusos*
   - *Segregación de la red de datos de las otras redes*
4. *Cifrado de datos*
5. *Copias de seguridad*
6. *Destrucción adecuada de dispositivos y eliminación de datos*
7. *Seguridad física de las instalaciones*

VOLVER AL INICIO DEL DOCUMENTO

ANEXO I. AGRADECIMIENTOS

Queremos agradecer a las siguientes personas o grupos de personas sus ideas para que esta Guía haya podido salir adelante:

- A Dña. Mabel Marijuán y Dña. Mª Jesús Marcos de la UPV/EHV por su documento "Cuaderno CEISH protección de datos" que nos ha servido de base para elaborar esta Guía.
- A Dña. Mónica Arenas Ramiro, Profesora Contratada Doctora de Derecho Constitucional de la Universidad de Alcalá.
- A la UCM por su documento “Guía básica protección datos en investigación”.
- A la UC3M por su documento “Guía básica sobre protección de datos para los investigadores en el desarrollo de la actividad investigadora”.
- Al Grupo de trabajo de Investigación de Delegados de Protección de Datos de la Sectorial de Secretarías Generales-CRUE por el borrador del documento “Guía sobre la protección de datos en los Proyectos de Investigación”.

VOLVER AL INICIO DEL DOCUMENTO

ANEXO II. ¿QUÉ ES UN DATO PERSONAL? DERECHOS A LA PROTECCIÓN DE DATOS Y CÓMO EJERCITARLOS. OBLIGACIONES EN EL TRATAMIENTO DE LOS DATOS PERSONALES

Para obtener más Información sobre esta temática, puedes ver la "Guía para el Ciudadano" elaborada por la Agencia Española de Protección de Datos (AEPD).

También puedes encontrar información en la Página Web de Protección de datos de la UAH (https://www.uah.es/protecciondedatos) en los Apartados "Definiciones", "Principios", "Derechos" y "Obligaciones".

VOLVER AL INICIO DEL DOCUMENTO

ANEXO III. DATOS DE MENORES

Para obtener más Información sobre esta temática puedes consultar los siguientes enlaces:

- La infografía "Información sobre consentimiento para tratar datos personales de menores de edad"
- Dentro del Apartado MENORES Y EDUCACIÓN de la web de la Agencia Española de Protección de Datos (AEPD) se pueden encontrar una variedad de Preguntas Frecuentes que pueden ser de utilidad para llevar a cabo la investigación, como:
  - ¿Cuál es la edad para que los menores puedan prestar consentimiento para tratar sus datos personales?
  - ¿Se pueden recabar y tratar datos personales de menores?
  - ¿Puede un menor de 14 años ejercitar los derechos contemplados en el RGPD?
  - ¿Se pueden tomar imágenes o grabar vídeos en eventos escolares?
  - ¿Dónde puedo obtener más información sobre el tratamiento de datos de menores?
  - En caso de separación, ¿tienen ambos progenitores derecho a recibir del centro educativo la misma información sobre el proceso formativo de sus hijos?

VOLVER AL INICIO DEL DOCUMENTO

ANEXO IV. INVESTIGACIÓN MÉDICA Y BIOMÉDICA

- Dentro del Apartado SALUD de la web de la Agencia Española de Protección de Datos (AEPD) se puede encontrar el siguiente enlace muy interesante para la INVESTIGACIÓN BIOMÉDICA:
  Consentimiento de participantes en un estudio de investigación biomédica (adultos y menores afectados por diferentes patologías) para la grabación de imágenes y audios y su posterior difusión
- Y en cuanto al Área de actuación de SALUD, la AEPD tiene recogida la siguiente información interesante para la Investigación (última actualización 13 de noviembre de 2023):
  - Tus derechos en relación con tus datos de salud
  - Guías, informes del Gabinete Jurídico y consultas de Delegados de Protección de Datos sobre salud
  - Investigación sanitaria y ensayos clínicos. Dentro de este epígrafe se podrá encontrar información de interés práctico, por ejemplo:
    - Código de Conducta regulador del tratamiento de datos personales en el ámbito de los ensayos clínicos y otras investigaciones clínicas y de la farmacovigilancia.
    - Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos (REC) y el Reglamento general de protección de datos (RGPD) [artículo 70, apartado 1, letra b)].
  - Protección de datos personales en la pandemia de COVID-19
  - Principales reclamaciones en materia de salud
  - Brechas de datos personales en el sector de la salud

VOLVER AL INICIO DEL DOCUMENTO

ANEXO V. TRANSFERENCIAS INTERNACIONALES

Dentro del Apartado TRANSFERENCIAS INTERNACIONALES de la web de la AEPD se pueden encontrar una variedad de Preguntas Frecuentes que pueden ser de utilidad para llevar a cabo la investigación, como:

- ¿Cuáles son los supuestos que contempla el RGPD para la realización de transferencias internacionales?
- ¿Qué países se consideran con un nivel adecuado a efectos del artículo 45 del RGPD?
- ¿Cuándo es necesario la autorización de la AEPD para realizar una transferencia internacional de datos?
- Y podrás encontrar más información sobre garantías para las transferencias de datos personales a terceros países u organizaciones internacionales en https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

VOLVER AL INICIO DEL DOCUMENTO

ANEXO VI. ANÁLISIS DE RIESGOS Y EVALUACIÓN DE IMPACTO EN EL TRATAMIENTO DE DATOS PERSONALES

Dentro del Apartado INNOVACIÓN Y TECNOLOGÍA de la web de la AEPD se pueden encontrar una variedad de "Herramientas básicas para el cumplimiento de la Responsabilidad Proactiva" establecida en el RGPD, y entre ellas, las que nos ayudarán a realizar un análisis de riesgos y una Evaluación de Impacto, si fuese necesario.

Como ya se ha comentado en los Apartados 14 y 15 de esta Guía, la AEPD ha puesto a disposición de los Responsables y de los Encargados del tratamiento de datos personales una serie de herramientas que nos ayuden a cumplir con la legislación vigente en materia de Protección.

Con el objetivo de ayudar en el análisis de riesgos orientado a determinar las medidas de seguridad, la AEPD ofrece indicaciones en la Guía Gestión del riesgo y evaluación de impacto en tratamientos de datos personales [junio 2021].

Del mismo modo, la AEPD ha puesto a disposición la herramienta FACILITA-RGPD a utilizar cuando se realice un tratamiento de datos personales de *escaso riesgo* para el cumplimiento del Reglamento General de Protección de Datos. No podrá utilizarse para tratamientos que impliquen un alto riesgo para los derechos y libertades de las personas, como datos de salud o tratamientos masivos de datos, entre otros.

En junio del 2023, la Agencia Española de Protección de Datos (AEPD) ha lanzado una nueva versión de su herramienta GESTIONA RGPD, orientada especialmente a pequeñas entidades públicas o privadas –que te puede servir de orientación en tu investigación-, y que permite gestionar los tratamientos, realizar la gestión de riesgos y, en su caso, dar soporte para la realización de las evaluaciones de impacto. "Gestiona RGPD" (AEPD) se ha rediseñado con un formato más intuitivo e incorpora las últimas directrices recogidas en las guías publicadas por la Agencia.

Además, en septiembre de 2023, la AEPD ha elaborado una nueva versión de la guía que contiene las "Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo" [junio 2023].

La AEPD también ha elaborado dos listados de aquellos tratamientos en los que:

- **NO** es necesario realizar una Evaluación de Impacto relativa a la Protección de datos https://www.aepd.es/sites/default/files/2019-12/ListasDPIA-35.5l.pdf [agosto 2019]
- **SI** es necesario realizar una Evaluación de Impacto relativa a la Protección de datos https://www.aepd.es/documento/listas-dpia-es-35-4.pdf [septiembre 2019]

Además de lo ya visto, en el Apartado INNOVACIÓN Y TECNOLOGÍA de la web de la AEPD también se puede encontrar la siguientes información:

- En el **Blog de la AEPD** podéis leer los siguientes *Post*:
  - ¿Conoces Gestiona? [enero 2020]
  - El enfoque de riesgos en el Reglamento [noviembre 2017]
- En **Modelos y formularios** se encuentran los siguientes documentos:
  - Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas [abril 2022]
  - Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado [marzo 2022]
  - Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa [febrero 2022]

VOLVER AL INICIO DEL DOCUMENTO

ANEXO VII. BIOMETRÍA

Dada la gran aplicación de la inteligencia artificial en la biometría, en el siguiente enlace se puede encontrar información de gran interés especifica de Inteligencia artificial y decisiones automatizadas.

- **Guías y Notas Técnicas**
  - Nota Técnica: 14 equívocos con relación a la identificación y autenticación biométrica [junio 2020]
- En el **Blog de la AEPD** podéis leer los siguientes *Post*:
  - Empleo de datos biométricos: Evaluación desde la perspectiva de protección de datos [julio 2022]

VOLVER AL INICIO DEL DOCUMENTO

ANEXO VIII. CIFRADO Y PRIVACIDAD

De igual forma, en el Apartado INNOVACIÓN Y TECNOLOGÍA de la web de la AEPD se encuentra información sobre esta temática.

- **Guías y Notas Técnicas**
  - Orientaciones para la validación de sistemas criptográficos en la protección de datos [mayo 2023]
- En el **Blog de la AEPD** podéis leer los siguientes *Post*:
  - Cifrado y Privacidad (V): la clave como dato personal [diciembre 2021]
  - Cifrado y Privacidad IV: Pruebas de conocimiento cero [noviembre 2020]
  - Cifrado y Privacidad III: Cifrado Homomórfico [junio 2020]
  - Cifrado y Privacidad II: El tiempo de vida del dato [enero 2020]
  - Cifrado y Privacidad: cifrado en el RGPD [noviembre 2019]

VOLVER AL INICIO DEL DOCUMENTO

ANEXO IX. OTROS ENLACES DE INTERÉS

Agencia Española de Protección de Datos

Autoridad Catalana de Protección de Datos

Autoridad Vasca de Protección de Datos

Consejo de Transparencia y Buen Gobierno

Oficina de Seguridad del Internauta

Instituto Nacional de Ciberseguridad

Centro Criptológico Nacional

Y la Página web de la Unidad de Protección de Datos de la UAH en donde hay mucha información y documentación que puede ser de vuestro interés, no sólo para llevar a cabo vuestra investigación, sino para vuestro trabajo del día a día. RECUERDA que, si tienes dudas, puedes ponerte en contacto con la Unidad de Protección de Datos de la Universidad, escribiendo tu consulta a protecciondedatos@uah.es

VOLVER AL INICIO DEL DOCUMENTO

ANEXO X. REGISTRO DOCUMENTAL

En el presente Anexo se incluyen los datos documentales relativos a esta Guía de Protección de Datos en Investigación de la Universidad de Alcalá. Recogiéndose la información relativa de la misma, como son las versiones del documento, quién lo ha elaborado y aceptado, a quién se ha distribuido el Documento y el control de cambios del mismo.

- **DOCUMENTO**

DOCUMENTO	
Título	Guía de Protección de Datos en Investigación de la Universidad de Alcalá
Fecha	Junio 2024
Versión	1.0

- **CONTROL DEL DOCUMENTO**

ELABORADO	ACEPTADO
Dña. Remedios Menéndez Calvo	Delegada de Protección de Datos de la Universidad de Alcalá
Dña. Mª Luisa Fuentes Pedroche	Jefa del Servicio de la Unidad de Protección de Datos de la Universidad de Alcalá

- **DISTRIBUCIÓN DEL DOCUMENTO**

DISTRIBUCIÓN DEL DOCUMENTO	
Nombre	**Área**
D. Miguel Rodríguez Blanco	Secretario General de la UAH
D. F. Javier de la Mata de la Mata	Vicerrector de Investigación y Transferencia de la Universidad de Alcalá

- **REGISTRO DE CAMBIOS**

REGISTRO DE CAMBIOS			
Versión	**Fecha**	**Autor**	**Motivo del cambio**
2.0			

VOLVER AL INICIO DEL DOCUMENTO