

Formación: Protección de datos en el ámbito de investigación

Impulsora del proyecto

D^a. Ana María Amorós
Directora Área Jurídica y de
Delegación de Protección de Datos

Objeto de los Pliegos

- ✓ Seguimiento y adaptación RGPD
- ✓ Designación de un DPD
- ✓ Revisión y adaptación al ENS

Empresa adjudicataria

Telefónica-Tech

Dpd@upv.es

Servicio_jurídico@upv.es

Gloria Martín – RGPD

Identificar las acciones
necesarias para actualizar la
implantación del RGPD y LOPD-
GDD

Borja Sendra – DPD

Atención consultas y
gestión de proyectos

I. Introducción: Concepto de dato personal y tipología de datos personales

Normativa aplicable

Principios de protección de datos en el ámbito de investigación

Evidencia del consentimiento

Roles de responsabilidad en el ámbito de investigación

Cuestiones prácticas a tener en cuenta

Medidas de seguridad: conservación de la información y tratamiento

I. Introducción: Concepto de dato personal y tipología de datos personales

Normativa aplicable

Principios de protección de datos en el ámbito de investigación

Evidencia del consentimiento

Roles de responsabilidad en el ámbito de investigación

Cuestiones prácticas a tener en cuenta

Medidas de seguridad: conservación de la información y tratamiento

¿Qué es un dato personal?

Persona física

*Información
relacionada
con la persona*

*¿Qué no es un dato
personal?*

*Persona
jurídica*

*Información
anónima*



¿Es un dato personal?

- *¿DNI?*
- *¿y el CIF de una empresa?*
- *¿una dirección IP?*
- *¿IMEI del teléfono?*
- *¿Matrícula de un coche?*
- *¿Datos de si estás vacunado en COVID?*
- *¿Grados de fiebre?*

Los datos personales: tipos

Datos no especialmente protegidos

Datos de identificación

Datos de contacto

Datos bancarios

Datos educativos

(...)

Datos especialmente protegidos

el origen étnico o racial,
las opiniones políticas,
las convicciones religiosas o filosóficas, o la afiliación
sindical,
y el tratamiento de datos genéticos, datos biométricos
dirigidos a identificar de manera unívoca a una persona
física,
datos relativos a la salud o datos relativos a la vida
sexual o las orientación sexuales de una persona física

***Está prohibido su tratamiento salvo
excepción***

Los datos personales: tipos

Datos no especialmente protegidos

Datos de identificación

Datos de contacto

Datos bancarios

Datos educativos

(...)

¿Datos de violencia de género?

Datos especialmente protegidos

el origen étnico o racial,
las opiniones políticas,
las convicciones religiosas o filosóficas, o la afiliación sindical,
y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física,
datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física

Está prohibido su tratamiento salvo excepción

Puedo estar tratando datos personales:



- Realizando encuestas o entrevistas
- Utilizando bases de datos
- Relacionándome con los propios sujetos de investigación

Investigación y datos especialmente protegidos

Una de las excepciones a la prohibición de tratar datos especialmente protegidos es que sea **necesario para una investigación científica o histórica**

Otra de las excepciones es que el interesado de su **consentimiento explícito**

Cuando se traten estos datos deberán adoptarse **especiales medidas técnicas y organizativas de seguridad**



I. Introducción: Concepto de dato personal y tipología de datos personales

Normativa aplicable

Principios de protección de datos en el ámbito de investigación

Evidencia del consentimiento

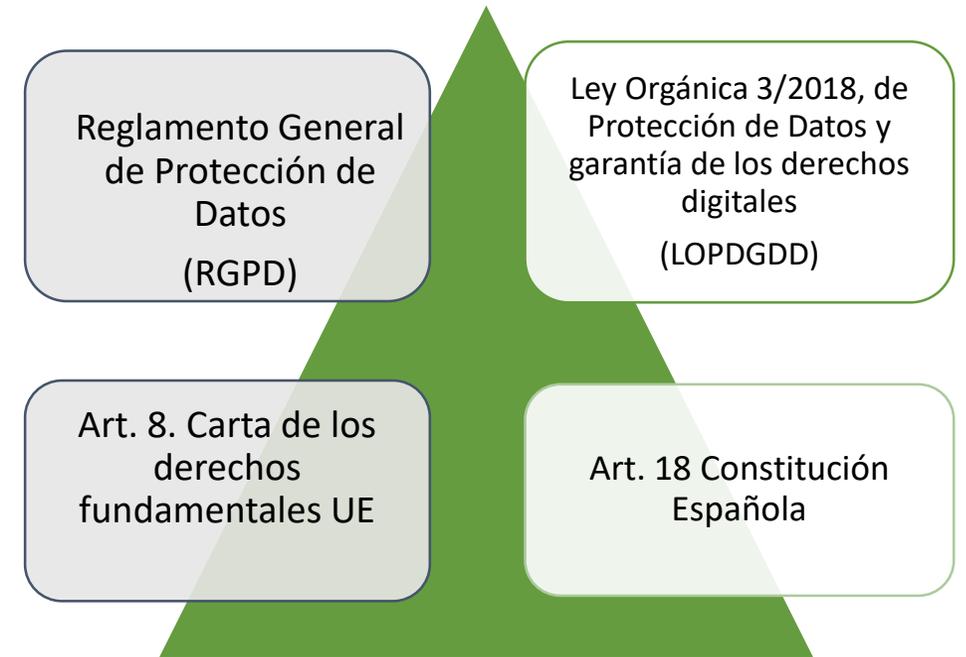
Roles de responsabilidad en el ámbito de investigación

Cuestiones prácticas a tener en cuenta

Medidas de seguridad: conservación de la información y tratamiento

¿Dónde se regula?

1978 Constitución Española art. 18	Íntimamente ligado con el derecho a la intimidad <i>“Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen (...) La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.</i>
STC 94/1998	Derecho fundamental a la protección de datos.
STC 254/1993 y 292/2000	Derecho autónomo e independiente



Normativa aplicable

¿Dónde se regula?

Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario

- Art. 2. Funciones del sistema universitario. “c) La Generación, desarrollo, difusión, transferencia e intercambio del conocimiento y la aplicabilidad de la investigación en todos los campos científicos, tecnológicos, sociales, humanísticos, artísticos y culturales.”
- Art. 3.3 “La autonomía universitaria garantiza la libertad de cátedra del profesorado, que se manifiesta en la libertad en la docencia, la investigación y el estudio”
- Art. 11.1 “La Investigación es una de las funciones fundamentales de las universidades”
- Art. 11.2 “La investigación, al igual que la docencia, es un derecho y un deber del personal docente e investigador. (...)”

Legislación de autonomía del paciente

- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica
- Legislación autonómica

Ley 14/2007, de 3 de julio, de Investigación Biomédica

Código de Conducta de FarmaIndustria

- <https://www.aepd.es/es/documento/codigo-conducta-farmaindustria-cc-0007-2019.pdf>

Normativa aplicable

INVESTIGACIÓN EN EL RGPD y LOPDGDD

Garantizar la
protección de los
datos personales

Poder tratar los datos
para investigaciones
científicas, sociales o
históricas que
impulsen la mejora de
la sociedad o aporten
beneficios a su
conjunto

Artículo 89.1 RGPD: “El tratamiento con fines de archivo en interés público, fines de **investigación científica o histórica** o fines estadísticos estará sujeto a las **garantías adecuadas**, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo”.

Artículo 89.2 RGPD. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos de los interesados si es probable que imposibiliten u obstaculicen gravemente el logro de los fines científicos y las excepciones sean necesarias para alcanzar esos fines.

DA decimoséptima LOPDGDD. Establece criterios para el tratamiento de datos en la investigación en salud, en investigaciones médicas y biomédicas.

Normativa aplicable

I.Introducción: Concepto de dato personal y tipología de datos personales

Normativa aplicable

Principios de protección de datos en el ámbito de investigación

Evidencia del consentimiento

Roles de responsabilidad en el ámbito de investigación

Cuestiones prácticas a tener en cuenta

Medidas de seguridad: conservación de la información y tratamiento

Todo tratamiento de datos personales realizado, debe cumplir con los siguientes PRINCIPIOS:

- 1.- **Licitud:** Tiene que estar **permitido** por la normativa. Por ejemplo, será lícito cuando el interesado haya dado su consentimiento.
- 2.- **Lealtad y transparencia:** Hay que **informar** adecuadamente a los interesados.
- 3.- **Minimización:** Se utilizarán los datos **justos y necesarios** para la finalidad que se persigue (serán adecuados, pertinentes y limitados a lo necesario).
- 3.- **Exactitud:** Los datos serán **exactos y actualizados** y deben rectificarse/suprimirse sin dilación.
- 4.- **Principio de limitación de la finalidad:** Los datos se recogen con **fines determinados y concretos** y no se tratan después de forma incompatible. En investigación se pueden **reutilizar** en investigaciones con fines compatibles.
- 5.- **Limitación del plazo de conservación:** **No** se tratan los datos por **más tiempo del necesario**.
- 6.- **Integridad y confidencialidad:** Hay que **proteger los datos** ante accesos no autorizados o ilícitos. Establecer medidas de seguridad técnicas y organizativas adecuadas.

*Responsabilidad
proactiva*

Cumplir

Demostrar que cumplo

Privacidad desde el diseño y por defecto

Este principio está regulado en el Artículo 25 RGPD y engloba dos:

Privacidad desde el diseño

- Hay que tener en cuenta el tratamiento de datos personales **desde el principio**, cuando se planifica la actividad de investigación.
- Desde el primer momento **se integrarán en el proyecto** las medidas para proteger los datos, que se aplicarán durante todo el proceso y cuando finalice.



Privacidad por defecto

- Se aplicarán **las medidas necesarias** para que, por defecto, se traten solo los mínimos datos y los exclusivamente necesarios.
- Se refiere a la cantidad de datos, extensión de su utilización, plazo de conservación y accesibilidad.

I. Introducción: Concepto de dato personal y tipología de datos personales

Normativa aplicable

Principios de protección de datos en el ámbito de investigación

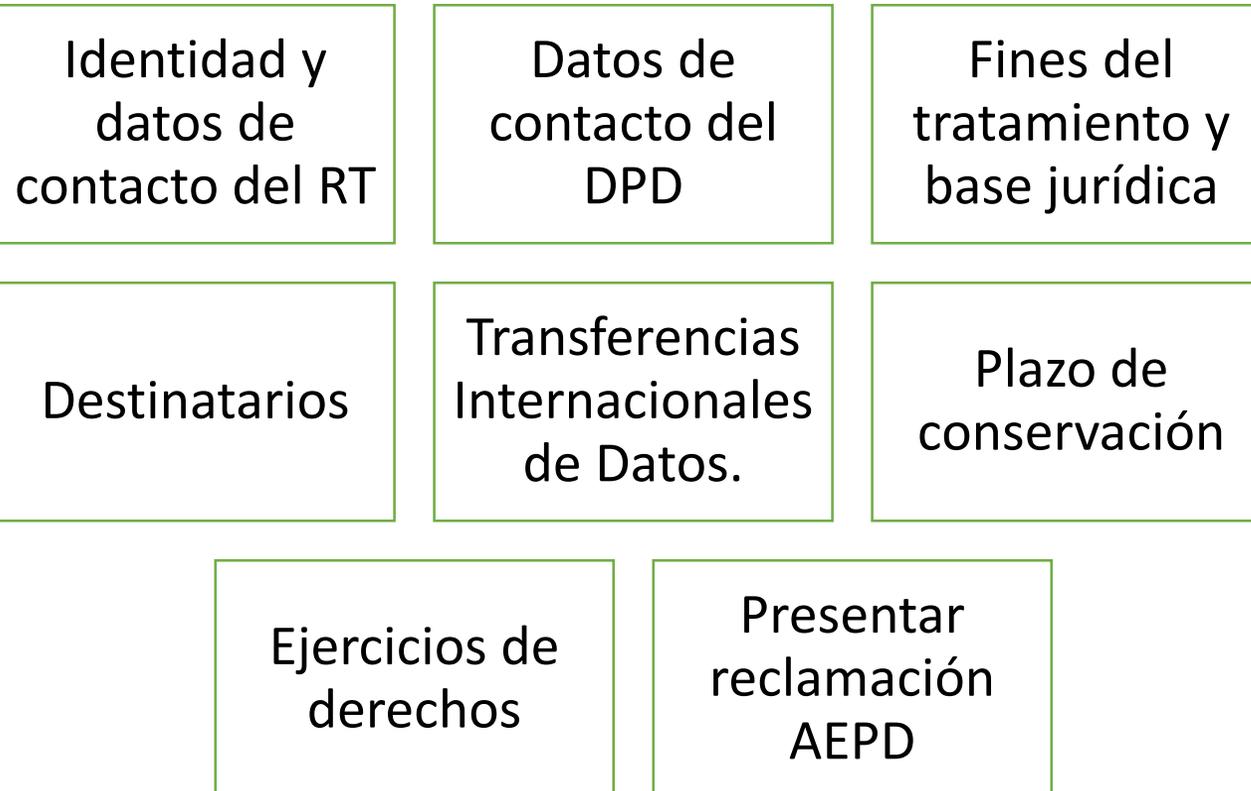
Evidencia del consentimiento

Roles de responsabilidad en el ámbito de investigación

Cuestiones prácticas a tener en cuenta

Medidas de seguridad: conservación de la información y tratamiento

¿De qué hay que informar ANTES ?



¿Dónde informamos?

Formularios
web

Formularios
internet

Correo
electrónico

Aplicaciones
web creadas

¿Cómo informamos?

Sistema de capas

Adaptando el
lenguaje al
destinatario

Conservando
evidencia de la
información
suministrada

El consentimiento informado

***Información
en primera
capa:***

RESPONSABLE DEL TRATAMIENTO

- La Universidad

FINALIDAD

- La investigación en concreto

EJERCICIO DE DERECHOS

- Cómo ejercitar los derechos de acceso, rectificación, oposición, supresión (“derecho al olvido”), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

INFORMACIÓN ADICIONAL

- Remisión a la política de privacidad en la página web

Legislación específica

Ley Investigación Biomédica

- Art. 4.1 Se respetará la libre autonomía de las personas que puedan participar en una investigación biomédica o que puedan aportar a ella sus muestras biológicas, para lo que será preciso que hayan **prestado previamente su consentimiento expreso y escrito una vez recibida la información adecuada.**
- La información se proporcionará **por escrito** y comprenderá la naturaleza, importancia, implicaciones y riesgos de la investigación, en los términos que establece esta Ley.
- La información se prestará a las personas con discapacidad en condiciones y formatos accesibles apropiados a sus necesidades.
- Si el sujeto de la investigación **no pudiera escribir**, el consentimiento podrá ser prestado por **cualquier medio admitido en derecho que permita dejar constancia de su voluntad.**
- Posibilidad de revocar el consentimiento

Ley de Autonomía del paciente

1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso.
 2. El consentimiento será verbal por regla general.
- Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente.

Legislación específica

DA 17ª LOPDGDD

- El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:
 - a) El interesado o, en su caso, su representante legal podrá **otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica**. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.
 - b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.
 - c) Se considerará lícita y compatible **la reutilización** de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.
- En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, **en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico**, y, en su caso, en la del promotor, **y notificar la existencia de esta información por medios electrónicos a los afectados**. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato. Para los tratamientos previstos en esta letra, **se requerirá informe previo favorable del comité de ética de la investigación**.

El consentimiento informado

Para poder tratar datos personales de los interesados de forma lícita, en general tendremos que **PEDIRLES SU CONSENTIMIENTO**.

Después de darles **toda la información** necesaria tienen que **ACEPTAR** participar en la investigación y que la Universidad trate para ello sus datos personales.



El interesado puede **RETIRAR EL CONSENTIMIENTO** en cualquier momento y debe poder hacerlo de forma sencilla

Cuidado, con:

NO VALE el consentimiento tácito

NO VALE usar casillas pre-marcadas para consentir

Tiene que ser una CLARA ACCIÓN AFIRMATIVA

Hay que DEMOSTRAR que nos lo dieron

- (Puede darse por escrito o verbalmente, pero que pueda demostrarse)



El consentimiento tiene que ser:

Libre

- (= sin limitación, condición o coacción; Código Civil, que no haya vicio en la manifestación de voluntad)

Específico

- (= se consiente o acepta en concreto un tratamiento/s y/o cesión de dato/s)

Inequívoco

- (= que no deja lugar a dudas → Acción positiva: marcar una casilla, desplazar una barra horizontalmente, ...)

Informado

- (= conocer el tratamiento antes de aceptar)

¿Quién debe conservar la evidencia del consentimiento?

El Responsable del Tratamiento

- A través del investigador
- Posibilidad de acreditar el consentimiento frente a terceros

El consentimiento informado

¿Se pueden tratar datos especialmente protegidos en una investigación (además de datos de salud)?

Sí

- Consentimiento
- El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el art. 89 sobre la base del derecho de la UE o de los EEMM, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado

El consentimiento informado

Reutilización de datos

- Es posible reutilizar los datos personales empleados en una investigación en **otra que tenga fines compatibles**, sin necesidad de una base jurídica diferente.
- Es decir, que si los datos personales son empleados para una investigación compatible con la original (mismo ámbito, fines, etc.), podrán usarse sin necesidad de volver a recabar el consentimiento de los interesados.

- Además, el RGPD considera compatible el tratamiento posterior con fines de **archivo** en interés público, de investigación científica, histórica o estadística.



Aunque existe esta presunción de compatibilidad, se considera necesario estudiar cada caso concreto y no ceder datos automáticamente

I. Introducción: Concepto de dato personal y tipología de datos personales

Normativa aplicable

Principios de protección de datos en el ámbito de investigación

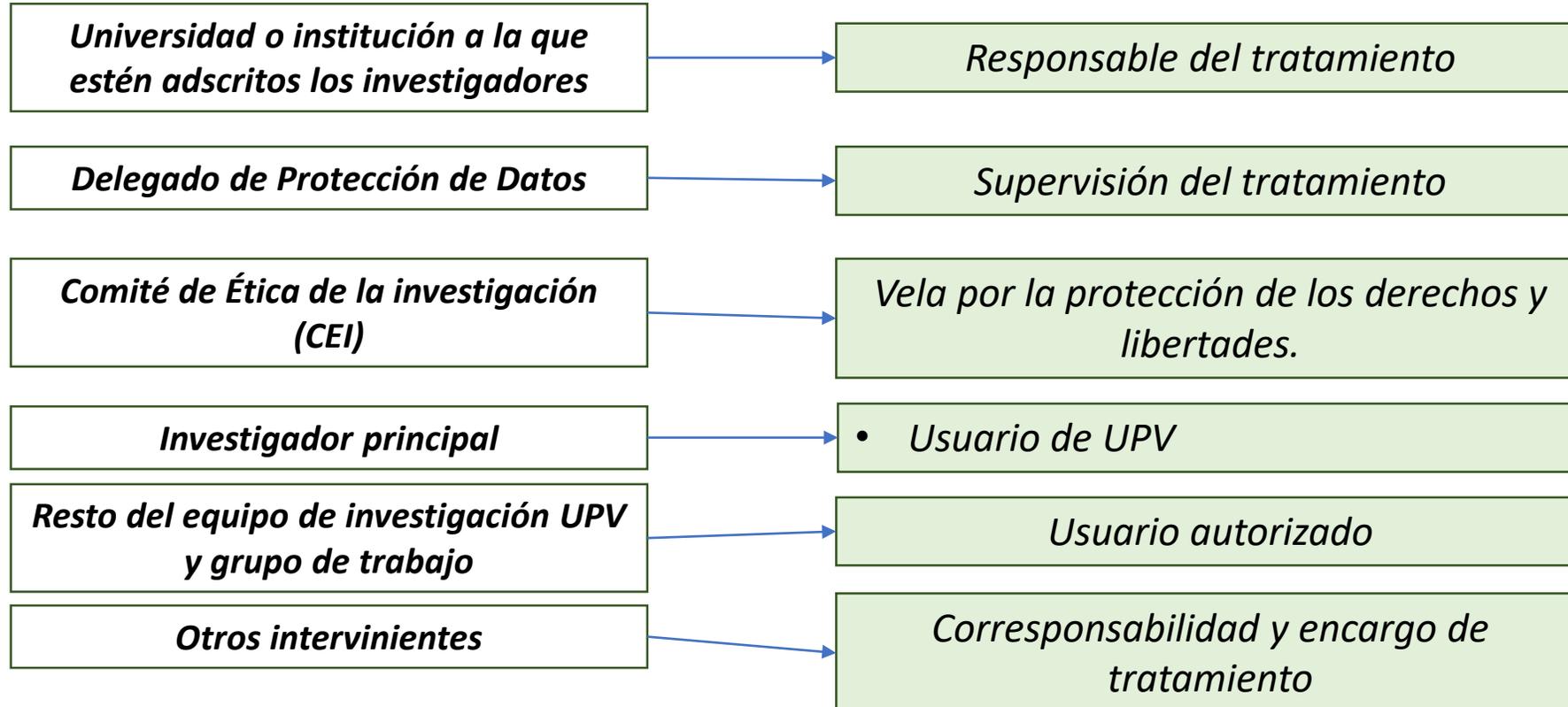
Evidencia del consentimiento

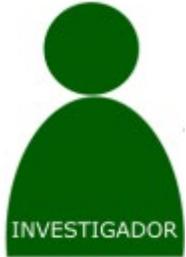
Roles de responsabilidad en el ámbito de investigación

Cuestiones prácticas a tener en cuenta

Medidas de seguridad: conservación de la información y tratamiento

¿Quién es qué?





Investigación en el marco de UPV

- La UPV es RT

Investigación privada ajena a UPV

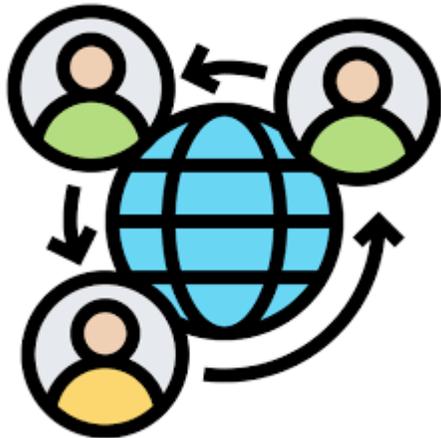
- El Investigador es RT

Grupos de investigación con otras entidades

- Entidad/es que decidan sobre los fines y medios del tratamiento es RT o Corresponsabilidad

Empresas o profesionales que sirven a la investigación

Encargados de tratamiento: son los profesionales, empresas o instituciones que gestionan tareas en nombre del responsable



¿Importa si el encargado está fuera de la UE?

Sí. Si las instituciones, empresas o profesionales están ubicados en un país no considerado seguro por las autoridades europeas en materia de protección de datos sería necesario seguir los requisitos establecidos en el capítulo V del RGPD para realizar la transferencia internacional de los datos con las adecuadas garantías para sus titulares.

Empresas o profesionales que sirven a la investigación

¿Qué obligaciones tenemos con los encargados?

- 1.- Procesos de validación del proveedor para garantizar que cumple principios RGPD
- 2.- Articular contrato encargo de tratamiento
- 3.- Revisión periódica de que sigue cumplimiento con los criterios de seguridad y protección de datos.

Roles de responsabilidad en el ámbito de investigación

Participación de otras organizaciones

Principio: transferencia del conocimiento. Art. 11.7 LOSU (...) “Las universidades impulsarán la formación de redes de investigación entre grupos, departamentos, centros, entidades y empresas

¿Quién asume el liderazgo de la investigación?

¿Se ceden datos entre órganos? ¿Cada uno trata los datos de sus propios interesados?

Roles de responsabilidad en el ámbito de investigación

I.Introducción: Concepto de dato personal y tipología de datos personales

Normativa aplicable

Principios de protección de datos en el ámbito de investigación

Evidencia del consentimiento

Roles de responsabilidad en el ámbito de investigación

Cuestiones prácticas a tener en cuenta

Medidas de seguridad: conservación de la información y tratamiento

Investigaciones con menores de edad

Ley Investigación Biomédica

- *2. Se otorgará el consentimiento por representación cuando la persona esté incapacitada legalmente o sea menor de edad, siempre y cuando no existan otras alternativas para la investigación.*
- *La prestación del consentimiento por representación será proporcionada a la investigación a desarrollar y se efectuará con respeto a la dignidad de la persona y en beneficio de su salud.*
- *Las personas incapacitadas y los menores participarán en la medida de lo posible y según su edad y capacidades en la toma de decisiones a lo largo del proceso de investigación*

Ley Autonomía del Paciente

- Se otorgará el consentimiento por representación en los siguientes supuestos (...) c) Cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor, después de haber escuchado su opinión, conforme a LOPJM
- Cuando se trate de menores emancipados o mayores de 16 años (que no tengan modificada su capacidad y que puedan comprender), no cabe prestar el consentimiento por representación

Investigaciones con menores de edad

LOPDGDD

- Art. 7. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de 14 años. Se exceptúa los supuestos en los que la ley exija la asistencia de los titulares de la patria potestad.
- El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela

Ojo → ¡Información a menores en términos comprensibles!

Transferencias internacionales de datos

¿Qué son?

¿Datos en el resto de países de la UE?

- Dentro de la UE no son TID

¿Se pueden realizar?

- Sí, pero debemos analizar la base que legitima

Reflexión previa:

- ¿Resulta necesario el tratamiento de datos de carácter personal entre instituciones?
- ¿Se pueden anonimizar con carácter previo a ser compartidas?
- ¿Resulta necesario utilizar tecnología?

Publicación de investigaciones

¿Qué NO podemos publicar?

- Datos que identifiquen al usuario investigado con la investigación.
- Por supuesto, no se publican datos relacionados con situaciones especialmente protegidas

¿Y si con ocasión de una publicación, nos interesa difundir a los investigados?

- Por ejemplo. Un medio de comunicación quiere hacerse eco de los resultados de la investigación y quieren entrevistar a una de las personas que haya sido objeto de investigación ¿le podemos pasar los datos de contacto? → No, si no tenemos el consentimiento expreso previo y por escrito (específicamente diseñado para tal fin)
- ¿Se puede utilizar la imagen o la voz de los investigados? → No, con carácter general. La voz y la imagen es un dato personal.

¡¡¡Fomento de la ciencia abierta!!!
¡Sin publicación de datos de carácter persona!

HORIZONTE EUROPA 21/27 – Proyectos Europeos

¿Qué es?

- Programa marco de investigación e innovación (I+I) de la Unión Europea (UE) para el período 2021 -2027.
- El **objetivo general del programa** es alcanzar un impacto científico, tecnológico, económico y social de las inversiones de la UE en I+I, fortaleciendo de esta manera sus bases científicas y tecnológicas y fomentando la competitividad de todos los Estados Miembros (EEMM).

Obligaciones: Plan de Gestión de Datos (PGD)

- El Horizonte Europa obliga a redactar y mantener un PGD.
- Cumplimiento de la normativa en materia de protección de datos (RGPD/GDPR).



Pilar 1 Excelencia científica

Consejo Europeo de
Investigación (ERC)

Acciones Marie Skłodowska-
Curie (MSCA)

Infraestructuras de Investigación



Pilar 2 Desafíos mundiales y competitividad industrial europea

Clústeres

- Salud
- Cultura, creatividad y sociedad inclusiva
- Seguridad civil para la sociedad
- Mundo digital, industria y espacio
- Clima, energía y movilidad
- Alimentación, bioeconomía, recursos naturales, agricultura y medio ambiente

Centro Común de Investigación
(JRC)



Pilar 3 Europa innovadora

Consejo Europeo de Innovación
(EIC)

Ecosistemas europeos de
innovación

Instituto Europeo de Innovación
y Tecnología (EIT)

Ampliar la participación y reforzar el Espacio Europeo de Investigación

Ampliar la participación y difundir la excelencia

Reformar y mejorar el sistema europeo de I+i

HORIZONTE EUROPA 21/27 – PGD

¿Qué es?

- **Un PGD describe el ciclo de vida de la gestión de los datos en la utilización, procesamiento y generación** para conseguir que los datos de investigación **sean localizables, accesibles, interoperables y reutilizables**, es decir, que sean **FAIR** (Findable, Accesible, Interoperable and Reusable). En resumen, indica **qué se va a hacer con los datos durante y después de finalizar la investigación**.

Contenido

- Determinar los requisitos de la entidad financiadora
- Identificar los datos que se utilizarán: tipología, procedencia, formatos, etc.
- Definir cómo se organizarán y gestionarán los datos: control de versiones, nombre de ficheros, etc.
- Explicar cómo se documentarán los datos
- Describir cómo se asegura la calidad de los datos
- Preparar una estrategia de almacenamiento y preservación de los datos
- Definir las políticas de datos del proyecto: propiedad intelectual, tratamiento de datos sensibles y personales, etc.
- Describir cómo se difundirán los datos: dónde, cuáles y cuándo se van a difundir, etc.
- Asignar roles y responsabilidades
- Preparar un presupuesto realista para la gestión de los datos

Ejercicios de derechos

¿Qué son y dónde se regulan?

- Derechos ARSOPL
- RGPD + LOPDGDD

RGPD. Art. 89.2

- Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuando esas excepciones sean necesarias para alcanzar esos fines.

1.LOPDGDD DA 17ª Letra e)

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

I. Introducción: Concepto de dato personal y tipología de datos personales

Normativa aplicable

Principios de protección de datos en el ámbito de investigación

Evidencia del consentimiento

Roles de responsabilidad en el ámbito de investigación

Cuestiones prácticas a tener en cuenta

Medidas de seguridad: conservación de la información y tratamiento

NO EXISTE EL RIESGO CERO



Artículo 89 Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las **garantías adecuadas**, con arreglo al presente Reglamento, para los **derechos y las libertades de los interesados**. Dichas garantías harán que se disponga de medidas técnicas y organizativas, **en particular para garantizar el respeto del principio de minimización** de los datos personales. Tales medidas podrán incluir la **seudonimización**, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.
2. (...)
3. 4. En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados

NO EXISTE EL RIESGO CERO



DA. 17 LOPDGDD

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en **salud pública y, en particular, biomédica** se procederá a:

1.º Realizar una **evaluación de impacto** que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las **normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica**.

3.º Adoptar, en su caso, medidas dirigidas **a garantizar que los investigadores no acceden a datos de identificación de los interesados**.

4.º Designar un representante legal establecido en la Unión Europea, conforme al **artículo 74 del Reglamento (UE) 536/2014, si el** promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, **biomédica** deberá ser sometido al **informe previo del comité de ética** de la investigación previsto en la **normativa sectorial**

MEDIDAS TÉCNICAS

- Seudonimización de la información.
- Cifrado de la información y de las comunicaciones.
- Credenciales de acceso físico y/o de acceso lógico.
- Mecanismos de atribución y control de permisos a usuarios.
- Empleo de antivirus y cortafuegos.
- Respuestas ante brechas de seguridad.
- Políticas de protección de seguridad de la red.
- Copias de seguridad, retención de copias de seguridad.
- Clasificación, conservación y recuperación de la información.
- Seguridad de los datos en el manejo de los medios de almacenamiento.
- Medidas de seguridad en locales (alarmas, videovigilancia, etc).

MEDIDAS ORGANIZATIVAS

- Formación del personal.
- Uso y actualización de credenciales de acceso físico y lógico.
- Copias de seguridad y respaldo. Protocolo.
- Actualización y supresión de datos. Protocolo.
- Registro de incidencias.
- DPD. Delegado de Protección de Datos.
- Realización periódica de auditorias.
- EIPD. Evaluación de Impacto Protección de Datos.
- Implantación de políticas de privacidad y protección de datos.
- Uso correo electrónico y de internet.
- Escritorios limpios.
- Destrucción de documentos.
- Protección de contraseñas.

La seudonimización

Datos seudonimizados: Son aquellos datos personales que ya no pueden atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable.



Anonimización: (LIB) proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere

Dato anónimo: dato registrado sin un nexo con una persona identificada o identificable

Desidentificación: eliminación de identificadores que identifican al interesado.

DA 17ª.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una **separación técnica y funcional** entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente **sean accesibles al equipo de investigación** cuando:

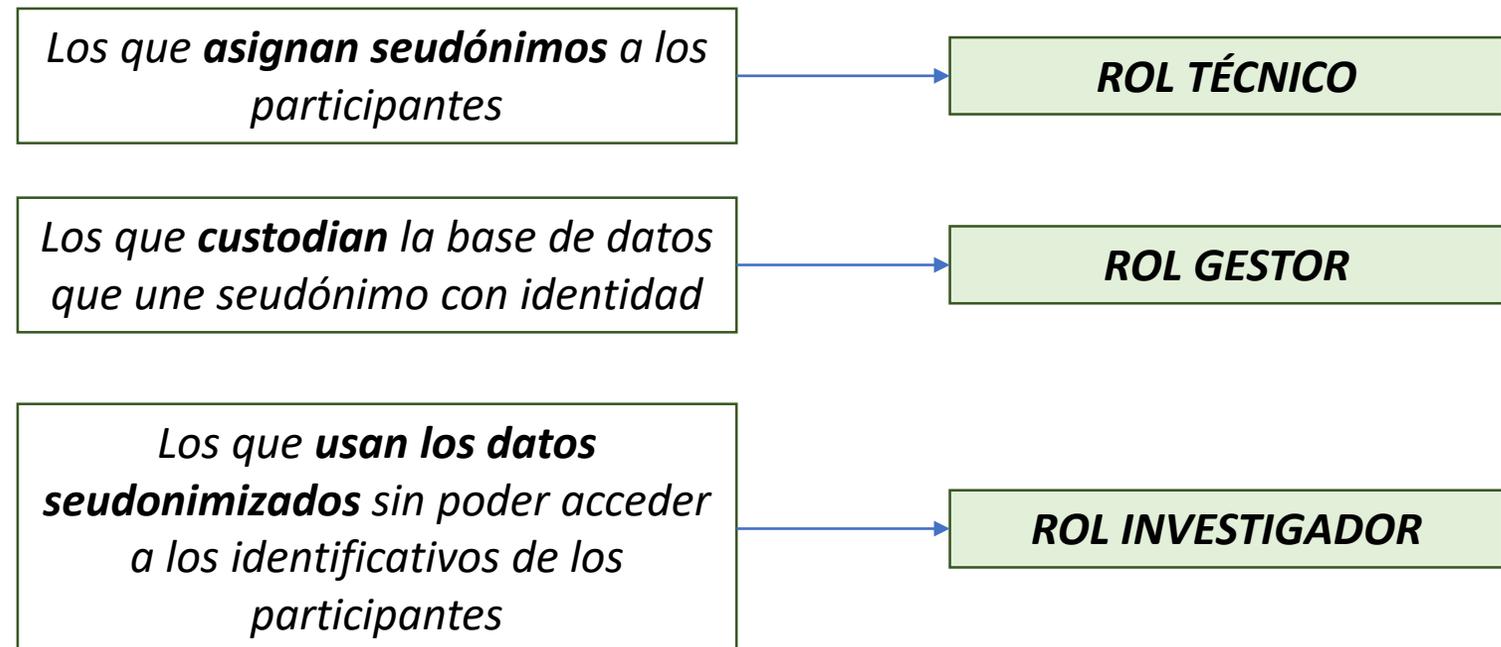
i) Exista un **compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.**

ii) Se adopten **medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.**

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

Tiene que haber **SEPARACIÓN TÉCNICA Y FUNCIONAL** entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

Tienen que asignarse **ROLES** y accesos a la información claramente definidos:



Datos o documentos cifrados



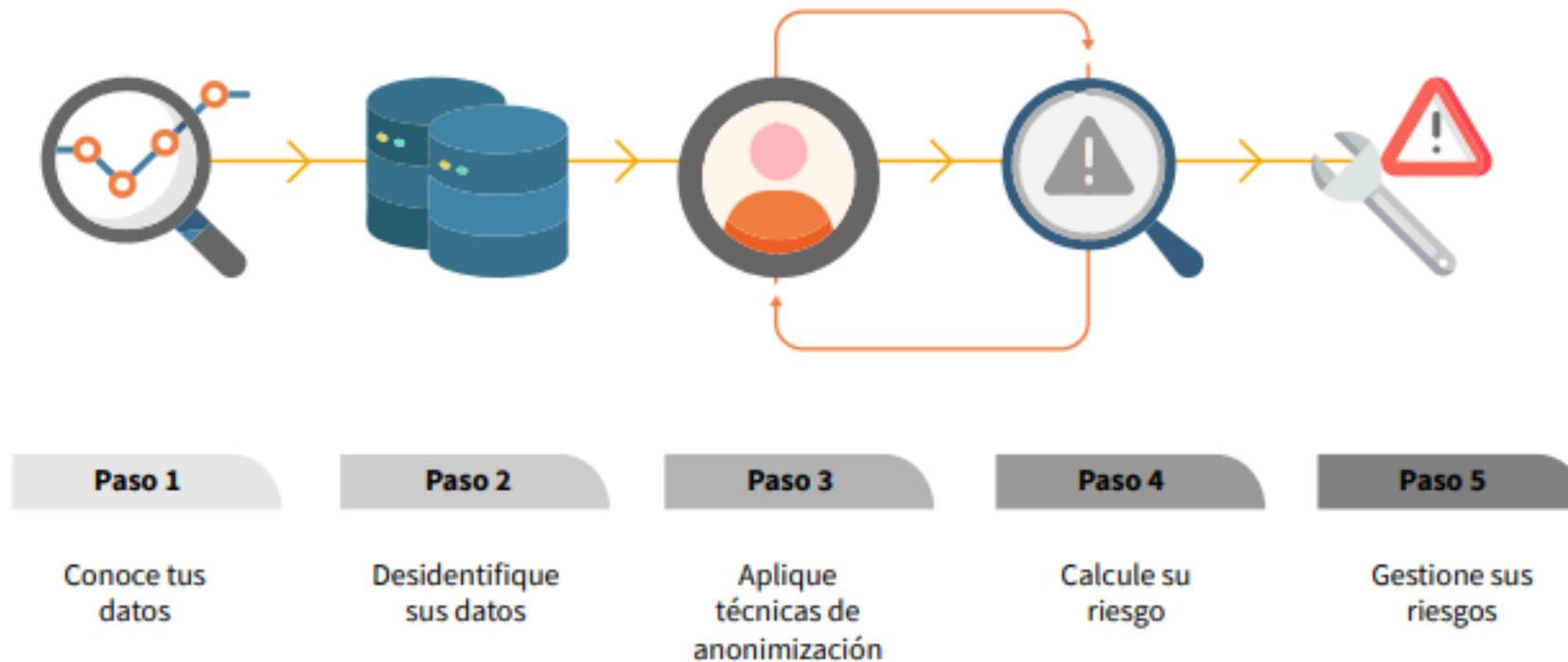
Se aplican técnicas de codificación de los mensajes o de los documentos de modo que sólo se puede comprender el contenido si se conoce la clave para su decodificación. Por ejemplo, enviar un documento con una clave de acceso

Guía Básica de Anonimización

Guía Básica de Anonimización – Autoridad de Singapur

<https://www.aepd.es/es/documento/guia-basica-anonimizacion.pdf>

Guía Básica de Anonimización



Medidas de Seguridad

Guía Básica de Anonimización

Técnicas de anonimización sugeridas para datos a nivel de registro

- **Supresión de registros:** la eliminación de un registro (es decir, una fila de datos, especialmente cuando dichos datos pueden contener valores de datos únicos que no se pueden anonimizar más).
- **Supresión de atributos:** la eliminación de un atributo de datos (es decir, una columna de datos, especialmente cuando dichos datos no son necesarios en el conjunto de datos y pueden contener valores de datos únicos que no se pueden anonimizar más).
- **Enmascaramiento de caracteres:** la sustitución de algunos caracteres del valor de datos por un símbolo coherente (por ejemplo, * o x). Por ejemplo, enmascarar un código postal implicaría cambiarlo de “28029” a “28xxx”.
- **Generalización:** La reducción de la granularidad de los datos (por ejemplo, mediante la conversión de la edad de una persona en un rango de edad). Por ejemplo, generalizar la edad de una persona de “26 años” a “25-29 años”.

- **Perturbación de datos:** Modificación de los valores en los datos agregando “ruido” a los datos originales (por ejemplo, valores aleatorios +/- a los datos). El grado de perturbación debe ser proporcional al rango de valores del atributo. Por ejemplo, la perturbación de los datos implicaría modificar los datos salariales de un individuo de “\$ 256,654” a “\$ 260,000” redondeando los datos a los \$ 10,000 más cercanos. Alternativamente, el salario del individuo se puede modificar a “\$ 250,554” restando un número aleatorio dentro de \$ 10,000 de su valor original.
- **Intercambio:** reorganización de los datos en el conjunto de datos de forma aleatoria de modo que los valores de los atributos individuales todavía se representan en el conjunto de datos, pero generalmente no corresponden a los registros originales.

Gestión de incidentes de seguridad

¿Qué es un incidente?

- Brechas de datos de carácter personal

Obligaciones

- Evaluar
- Notificar a la AEPD
- Notificar a los interesados

¿Qué se necesita?

- Tomar en serio las medidas de seguridad
- Notificar a Dpd@upv.es tan pronto como se conozcan.

Caso Pràctico

1. La UPV desarrolla una investigación financiada por el plan Horizonte Europa.
2. Se tratan datos de pacientes de forma no anonimizada: Datos relativos a la salud + datos identificativos.
3. Se desarrolla una aplicación para el análisis de los datos.
4. Se utilizan softwares de gestión y análisis de datos para algunas tareas.
5. Una vez analizados los datos se guardan los resultados de forma anonimizada para posibles futuros proyectos de investigación.

PGD

GUÍA - Formulario
Proyectos
Investigación Docente

Formulario Proyectos
Investigación Docente



2. Datos a rellenar para TODOS los proyectos con tratamiento de datos

2.1 Especifique los datos personales utilizados para el proyecto y la finalidad perseguida con estos.

2.2 Especifique el origen de proveniencia de los datos ¿Los datos provienen del paciente directamente o los facilita algún tercero (hospitales, organismos públicos o cualquier otro distinto al propio paciente)?

Por el participante Por el hospital u otro organismo público Otros (especificar)

2.3 ¿Existe el consentimiento expreso (documentado) para el tratamiento de sus datos personales?

SI NO

2.4 ¿Los datos están pseudonimizados o anonimizados (entendiendo como tal que no sea posible la identificación de la persona titular de los mismos)?

NO Sí, pseudoanonimizados Sí, anonimizados

Si la respuesta es afirmativa, justifique el proceso de anonimización o pseudonimización seguido.

2.5 ¿Se utiliza alguna herramienta o software ajeno a la UPV para su tratamiento (entendiendo como tal cualquier programa informático en el que se depositen los datos personales recabados y que sea ajeno a la UPV)?

SI NO

En caso afirmativo, especifique la herramienta utilizada

2.6 ¿Algún tercero (ajeno al equipo de investigación) tendrá acceso a los datos personales recabados?

SI NO

En caso afirmativo, justifique su respuesta

2.7 ¿Se informa al paciente sobre el tratamiento de sus datos personales y la posibilidad de ejercer sus derechos al recoger su consentimiento?

SI NO

En caso afirmativo, se debe añadir alguna evidencia de cláusula informativa para su posterior valoración.