

AYUDA PARA RELLENAR EL FORMULARIO DE REGISTRO DE TRATAMIENTO DE DATOS PERSONALES

Contenido

Inicio	2
1. Responsable del tratamiento	3
2. NOMBRE DEL TRATAMIENTO	4
3. FINALIDAD DEL TRATAMIENTO DE DATOS.....	5
4. LEGITIMACIÓN DEL TRATAMIENTO.....	10
5. ESTRUCTURA BÁSICA Y DESCRIPCIÓN DE LOS TIPOS DE DATOS DE CARÁCTER PERSONAL INCLUIDOS.....	11
6. FINALIDAD Y CARACTERÍSTICAS DEL TRATAMIENTO	13
7. CATEGORIAS DE INTERESADOS	15
8. PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA DE LOS DATOS	16
9. CESIÓN O COMUNICACIÓN DE DATOS.....	17
10. TRANSFERENCIAS INTERNACIONALES DE DATOS	18
11. ENCARGADOS DE TRATAMIENTO.....	19
12. CORRESPONSABLES DE TRATAMIENTO	19
13. DERECHOS DE LOS INTERESADOS	20
14. DISPONIBILIDAD, INTEGRIDAD, CONFIDENCIALIDAD, RESILIENCIA	21
14.1 Capacidad para preservar la Disponibilidad de los datos personales frente a la destrucción o pérdida de los datos personales.....	21
14.2 Capacidad para preservar la Integridad de los datos personales frente a su alteración accidental o ilícita.....	22
14.3 Capacidad para preservar la Confidencialidad de los datos personales frente a su comunicación o acceso no autorizados	22
14.4 Capacidad para preservar la Resiliencia de los datos personales en caso de sufrir incidente físico o técnico.....	22
15. SISTEMAS,SEGURIDAD Y MEDIOS DE TRATAMIENTO EN PROYECTOS DE INVESTIGACIÓN .	24
15.1. Describir los sistemas de información utilizados para el tratamiento de los datos personales	24
15.2. Papel.....	24
15.3 Electrónico.....	24
15.4. Disponibilidad.....	25
15.5 Integridad	25
15.6 Confidencialidad.....	25
15.7. Medios para el tratamiento de datos personales en proyectos de investigación	26

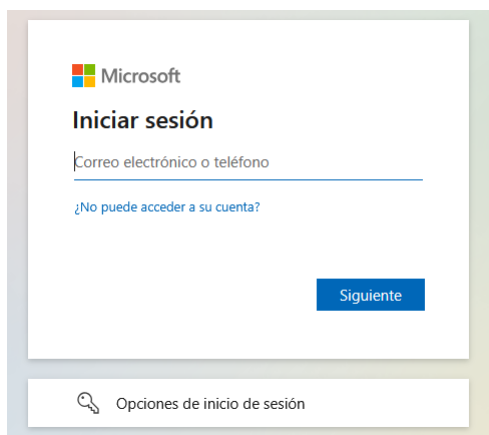
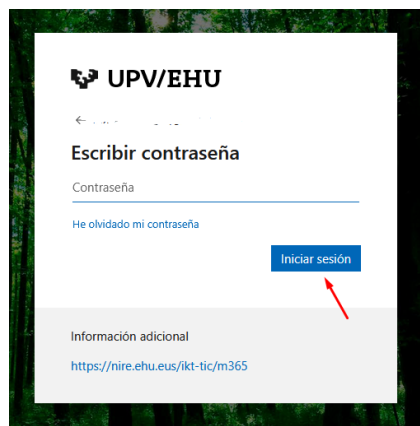
16. EVALUACIÓN DE IMPACTO (rellenar sólo si el tratamiento lo requiere) 26

Inicio

Accedemos a la **siguiente** url: Accedemos al formulario en la url:

<https://forms.office.com/e/qcvjTuk901>

Si no estamos ya dentro, introducimos el correo electrónico y nuestra contraseña:

The image shows the Microsoft login interface. At the top is the Microsoft logo. Below it, the text "Iniciar sesión" is displayed. There is a text input field labeled "Correo electrónico o teléfono". Below the field is a link that says "¿No puede acceder a su cuenta?". At the bottom right of the main area is a blue button labeled "Siguiente". At the very bottom, there is a link with a magnifying glass icon and the text "Opciones de inicio de sesión".The image shows the UPV/EHU login interface. At the top is the UPV/EHU logo. Below it, the text "Escribir contraseña" is displayed. There is a text input field labeled "Contraseña". Below the field is a link that says "He olvidado mi contraseña". At the bottom right of the main area is a blue button labeled "Iniciar sesión", with a red arrow pointing to it. At the bottom, there is a section titled "Información adicional" with a link: <https://nire.ehu.eus/ikt-tic/m365>.

Y se nos abre la primera pantalla del formulario, donde se nos permite seleccionar el idioma,:

The image shows the first screen of a Microsoft 365 form titled "DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL". At the top right, there is a language selector dropdown menu set to "Español (España, alfab...)" with a red arrow pointing to it. Below the title, there is a message: "Hola, MAREN. Cuando envíe este formulario, el propietario verá su nombre y dirección de correo electrónico." Below this, there are two text input fields: "Teléfono de contacto del solicitante" and "Número telefónico para contactar en caso de ser necesario". Below the second field is a text input field labeled "Escriba su respuesta". At the bottom left is a green button labeled "Siguiente". At the bottom right is a progress indicator showing "Página 1 de 17". At the very bottom, there is the Microsoft 365 logo and a disclaimer: "Este contenido lo creó el propietario del formulario. Los datos que envíe se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña." Below the disclaimer are links for "Microsoft Forms", "Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial", "Crear mi propio formulario", "Privacidad y cookies", and "Términos de uso".

En esta primera pantalla pondremos el número de teléfono móvil de la persona que está haciendo la solicitud, para el caso de que el tipo de tratamiento lo requiera el delegado de protección de datos se ponga en contacto con el solicitante. Lugo pulsamos en el botón de "siguiente":

Español (España, alfab...

...

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

Hola, MAREN. Cuando envíe este formulario, el propietario verá su nombre y dirección de correo electrónico.

Teléfono de contacto del solicitante

Número telefónico para contactar en caso de ser necesario

654673890

Siguiente

Página 1 de 17

Microsoft 365

Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial [Crear mi propio formulario](#)

Privacidad y cookies | Términos de uso

1. Responsable del tratamiento

A continuación metemos los datos de la persona contratada por la UPV/EHU que será responsable del tratamiento. los **campos marcados con asterisco rojo** a lo largo del formulario serán **siempre de respuesta obligatoria**. La persona responsable interna del tratamiento del tratamiento debe ser alguien con contrato en la UPV/EHU. En TFM, TFG o Tesis Doctorales serán usualmente las personas responsables de tutelar dichos trabajos. En el resto de proyectos de investigación la persona investigadora principal.

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

* Obligatorio

1. Responsable del tratamiento

Personal de la UPV/EHU responsable de la declaración de este tratamiento de datos

DNI *

Escriba su respuesta

Nombre y apellidos *

Escriba su respuesta

PUESTO / CARGO *

Escriba su respuesta

TELÉFONO *

Escriba su respuesta

EMAIL *

Escriba su respuesta

[Atrás](#) [Siguiente](#)

Página 2 de 17

Se puede ver el progreso completo del formulario en la parte inferior, no en todos los tratamientos habrá que rellenar todas las pantallas:

EMAIL *

juanzz.garcia@ehu.eus

[Atrás](#) [Siguiente](#)

Página 2 de 17

2. NOMBRE DEL TRATAMIENTO

Pulsamos en siguiente y nos aparece la siguiente sección, Elija un nombre breve para el tratamiento que lo definan, en proyectos de investigación es conveniente que coincida con el declarado en la memoria para el comité de ética:

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

* Obligatorio

2. NOMBRE DEL TRATAMIENTO

Título con el que se registrará el tratamiento, si es un proyecto de investigación conviene que coincida con el título del mismo

TÍTULO *

PSORIASIS

Atrás Siguiente

Página 3 de 17

Microsoft 365

Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial [Crear mi propio formulario](#)

[Privacidad y cookies](#) | [Términos de uso](#)

En todo momento **puede ir hacia atrás**, incluso, dependiendo del tipo de navegador **los datos** ya rellenados en el formulario, **no se perderán** aunque reinicie el ordenador.

3. FINALIDAD DEL TRATAMIENTO DE DATOS

Tras pulsar en “siguiente” debemos especificar la finalidad del tratamiento de datos. Describa la finalidad del proyecto brevemente, como en este ejemplo. No describa cómo se va a hacer, sino que se pretende hacer. Evite poner nombres de personas: frases del estilo "dentro de la Tesis Doctoral de Margarita Dosantos..."

Español (España, alfab...

...

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

* Obligatorio

3. FINALIDAD DEL TRATAMIENTO DE DATOS

Descripción breve de para qué exactamente se recopilan los datos personales

FINALIDAD *

ESTUDIO DE LA PSORIASIS EN SUS PRIMERAS FASES DE APARICIÓN. LA FINALIDAD ES EL ESTABLECIMIENTO DE CONCLUSIONES QUE PERMITAN ABRIR NUEVAS VÍAS DE INVESTIGACIÓN PARA LA BÚSQUEDA DE TRATAMIENTOS MÁS EFICACES.

Es un tratamiento permanente e indefinido (es aconsejable poner NO para no tener otros problemas, marcar SI solo en caso estrictamente necesario) *

☒ NO

☐ SI

Atrás

Siguiente

Página 4 de 17

Microsoft 365

Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial [Crear mi propio formulario](#)

Privacidad y cookies | Términos de uso

Como se señala con la flecha, es conveniente establecer una fecha de fin de uso de los datos, si no se pueden poner pegas a nivel de delegado de protección de datos, así que solo se debe marcar SI en caso estrictamente necesarios.

🌐 Español (España, alfab... 🗖 ...

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

* Obligatorio

3. FINALIDAD DEL TRATAMIENTO DE DATOS 🗖

Descripción breve de para qué exactamente se recopilan los datos personales

FINALIDAD * 🗖

ESTUDIO DE LA PSORIASIS EN SUS PRIMERAS FASES DE APARICIÓN. LA FINALIDAD ES EL ESTABLECIMIENTO DE CONCLUSIONES QUE PERMITAN ABRIR NUEVAS VÍAS DE INVESTIGACIÓN PARA LA BÚSQUEDA DE TRATAMIENTOS MÁS EFICACES.

Es un tratamiento permanente e indefinido (es aconsejable poner NO para no tener otros problemas, marcar SI solo en caso estrictamente necesario) * 🗖

☒ NO

☐ SI

ELIJE LA FECHA EN QUE LOS DATOS YA NO SERÁN NECESARIOS (Los consentimientos informados, si los hay deben guardarse 5 años después de esa fecha) * 🗖

Especifique la fecha (d/M/yyyy) 🗖

marzo 2025 ⬆ ⬇ ✕


lun.	mar.	mié.	jue.	vie.	sáb.	dom.	
24	25	26	27	28	1	2	🗖
3	4	5	6	7	8	9	
10	11	12	13	14	15	16	
17	18	19	20	21	22	23	
24	25	26	27	28	29	30	
31	1	2	3	4	5	6	

Ir a hoy

A continuación nos pide el tipo de tratamiento de datos: **Gestión** es para cuestiones administrativas y de gestión, **Investigación** es para proyectos de investigación (Incluyendo innovación educativa) y **difusión y eventos** es para eventos y difusión en general (congresos, difusión en redes sociales...).

En el caso de seleccionar INVESTIGACIÓN nos solicita el tipo de tratamiento de investigación:


14/06/2020

TIPO DE TRATAMIENTO * 

☒ INVESTIGACIÓN

☐ GESTIÓN

☐ DIFUSIÓN Y EVENTOS

TIPO DE INVESTIGACIÓN * 

☐ **TI0740- INVESTIGACIÓN BÁSICA SIN DATOS ESPECIALMENTE PROTEGIDOS.** Únicamente uso de Datos de carácter identificativo, de características personales, de circunstancias sociales, académicos y profesionales, detalle de empleo, económico-financieros...

☐ TI0741- INVESTIGACIÓN **CON DATOS ESPECIALMENTE PROTEGIDOS** (Salud, Ideología u opiniones políticas, religión, afiliación sindical, Creencias, origen racial, biométricos, datos genéticos, fines policiales...)

☐ TI0743- INVESTIGACIÓN **CON DATOS DE COLECTIVOS VULNERABLES** (Niños menores de 14, ancianos, discapacitados, personas en riesgo de exclusión social...)


☐ TI0742- INVESTIGACIÓN **CON DATOS PROCEDENTES DEL DEL BIOBANCO VASCO**

☐ TI0739- **INNOVACIÓN EDUCATIVA**

[Atrás](#) [Siguiente](#)

Página 4 de 17

En caso de seleccionar “TI0742- INVESTIGACIÓN CON DATOS PROCEDENTES DEL DEL BIOBANCO VASCO” o “TI0739- INNOVACIÓN EDUCATIVA” el formulario terminará:

TIPO DE INVESTIGACIÓN * 

☐ **TI0740- INVESTIGACIÓN BÁSICA SIN DATOS ESPECIALMENTE PROTEGIDOS.** Únicamente uso de Datos de carácter identificativo, de características personales, de circunstancias sociales, académicos y profesionales, detalle de empleo, económico-financieros...

☐ TI0741- INVESTIGACIÓN **CON DATOS ESPECIALMENTE PROTEGIDOS** (Salud, Ideología u opiniones políticas, religión, afiliación sindical, Creencias, origen racial, biométricos, datos genéticos, fines policiales...)

☐ TI0743- INVESTIGACIÓN **CON DATOS DE COLECTIVOS VULNERABLES** (Niños menores de 14, ancianos, discapacitados, personas en riesgo de exclusión social...)

☒ TI0742- INVESTIGACIÓN **CON DATOS PROCEDENTES DEL DEL BIOBANCO VASCO**

☐ TI0739- **INNOVACIÓN EDUCATIVA**

[Atrás](#) [Enviar](#)

Página 4 de 17

En el resto de los casos seguimos adelante.

Y nos pide que seleccionemos

EXTENSION GEOGRAFICA DEL TRATAMIENTO (Ámbito territorial del proyecto)


MEDIOS DEL TRATAMIENTO: Aquí se presentan tres opciones: físicos (papel, grabaciones analógicas, fotografías no digitales...), digitales (grabaciones digitales, ficheros informáticos...)

o mixtos (físicos + digitales) Tenga en cuenta que el consentimiento informado en papel constituye un medio físico.)

EL TRATAMIENTO DE HACE DE MANERA (Hay tres opciones posibles:

1. **Pseudonimizada** (reversible): es la más recomendable. Se asigna un código a los participantes de manera que el tratamiento automatizado se hace sin conocer la identidad de los participantes, pero llegado el caso, se puede facilitar el ejercicio de los derechos mencionados en el párrafo anterior.
2. Disociada (irreversible): Los datos proporcionados por la persona participante se disocian de manera que no hay manera de saber a quien pertenecen. La ventaja de esta manera de proceder es que garantiza un total anonimato. El inconveniente es que no podemos dar cauce a los derechos de los participantes (Acceso, Rectificación, Limitación, Oposición, Portabilidad y Supresión)
3. Sin medidas de protección de la identidad: se tratan los datos sabiendo en todo momento a quién pertenecen. Es la manera menos recomendable de hacerlo, pero a veces resulta inevitable.


NUMERO DE PERSONAS AFECTADAS: Rango de personas reclutadas para el proyecto

EXTENSION GEOGRAFICA DEL TRATAMIENTO * 

☒ REGIONAL

☐ NACIONAL


☐ INTERNACIONAL

MEDIOS DEL TRATAMIENTO * 

☐ DIGITAL (Electrónico)

☐ FISICO (Papel)


☒ MIXTO (Físico y Digital)

EL TRATAMIENTO SE HACE DE MANERA * 

☒ PSEUDONIMIZADA (Reversible)

☐ DISOCIADA (No reversible)

☐ SIN MEDIDAS DE PROTECCIÓN DE LA IDENTIDAD


NUMERO DE PERSONAS AFECTADAS * 

☒ 1-10000

☐ 10001-100000

☐ > 100000

[Atrás](#) [Siguiente](#)

Página 4 de 17 

Rellenamos la siguiente sección:

4. LEGITIMACIÓN DEL TRATAMIENTO

En un proyecto de investigación con seres humanos, la legitimación del tratamiento es casi siempre el consentimiento de las personas interesadas. El resto de títulos de legitimación implica que no es necesario el consentimiento de las personas interesadas y esto suele ser excepcional, pero no imposible.

4.1 Si ha elegido en el apartado anterior algún título de legitimación distinto del consentimiento informado, indique aquí cuáles son las leyes o regulaciones que le permiten recabar y tratar datos personales sin el consentimiento de sus titulares. **No indique el RGPD o la LOPDGDD, que son comunes a cualquier tratamiento de datos personales.**

4.2 No rellenar este apartado. De momento la UPV/EHU no ha elaborado ningún código de conducta ni se ha adherido a ninguno existente.

Español (España, alfab...

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

5. ESTRUCTURA BÁSICA Y DESCRIPCIÓN DE LOS TIPOS DE DATOS DE CARÁCTER PERSONAL INCLUIDOS

Describir aquí los datos personales que se pueden usar

5.1 DATOS ESPECIALMENTE PROTEGIDOS

- ☐ IDEOLOGÍA U OPINIONES POLÍTICAS
- ☐ AFILIACIÓN SINDICAL
- ☐ RELIGIÓN U OPINIONES RELIGIOSAS
- ☐ CREENCIAS O CREENCIAS FILOSÓFICAS
- ☐ ORIGEN RACIAL O ÉTNICO
- ☒ SALUD
- ☐ VIDA SEXUAL U ORIENTACIÓN SEXUAL
- ☐ VIOLENCIA DE GÉNERO Y MALOS TRATOS
- ☐ BIOMÉTRICOS
- ☐ DATOS GENÉTICOS QUE PROPORCIONAN UNA INFORMACIÓN ÚNICA SOBRE LA FISIOLOGÍA O LA SALUD DEL INTERESADO OBTENIDAS DEL ANÁLISIS DE UNA MUESTRA BIOLÓGICA
- ☐ DATOS SOLICITADOS PARA FINES POLICIALES SIN CONSENTIMIENTO DE LAS PERSONAS AFECTADAS
- ☐ DATOS RELATIVOS A CONDENAS Y DELITOS PENALES
- ☐ DATOS RELATIVOS A INFRACCIONES ADMINISTRATIVAS

Marque en este apartado cuantos datos vaya a recabar. Si no aparecen en la lista, utilice el campo otros, como en este ejemplo. No olvide marcar, **si recaba consentimientos informados, al menos "NOMBRE Y APELLIDOS" y "FIRMA/FIRMA DIGITALIZADA"**

Datos de carácter identificativo ☐

- ☒ DNI/NIF
- ☐ N° SS / MUTUALIDAD
- ☒ NOMBRE Y APELLIDOS
- ☐ DIRECCIÓN (POSTAL, ELECTRÓNICA)
- ☒ TELÉFONO
- ☒ FIRMA/HUELLA DIGITALIZADA
- ☐ IMAGEN
- ☐ VOZ
- ☐ MARCAS FÍSICAS
- ☐ N° REGISTRO PERSONAL
- ☐ FIRMA ELECTRÓNICA
- ☒ FOTOGRAFÍAS LESIONES


Datos de características personales ☐

- ☐ DATOS DE ESTADO CIVIL
- ☒ DATOS DE FAMILIA
- ☐ FECHA DE NACIMIENTO
- ☐ LUGAR DE NACIMIENTO
- ☒ EDAD
- ☒ SEXO

6. FINALIDAD Y CARACTERÍSTICAS DEL TRATAMIENTO


En el punto 6.1 se establecen las características del tratamiento, la mayoría de estas opciones no son aplicables a proyectos de investigación

Marque la tipificación que corresponda. La finalidad de los proyectos de investigación son "Fines científicos, históricos o estadísticos" y si acaso "publicaciones" (ver página siguiente). Raramente suelen ser otras opciones en proyectos de investigación, y sólo cuando el equipo de investigación es encargado o corresponsable de tratamiento, pudiera tener una finalidad distinta. Si se diera éste último caso, se puede consultar con el Delegado de Protección de Datos.

Tipificación correspondiente a la finalidad - FINALIDADES VARIAS 

- ☐ PROCEDIMIENTOS ADMINISTRATIVOS
- ☐ REGISTRO ENTRADA Y SALIDA DE DOCUMENTOS
- ☐ OTROS REGISTROS ADMINISTRATIVOS
- ☐ ATENCIÓN AL CIUDADANO
- ☐ CONCESIÓN Y GESTIÓN DE PERMISOS, LICENCIAS Y AUTORIZACIONES
- ☐ SEGURIDAD Y CONTROL DE ACCESO A EDIFICIOS
- ☒ **PUBLICACIONES**
- ☒ **FINES CIENTÍFICOS, HISTÓRICOS O ESTADÍSTICOS**
- ☐ GESTIÓN SANCIONADORA
- ☐ GESTIÓN DE ESTADÍSTICAS INTERNAS
- ☐ PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN
- ☐ Otras

[Atrás](#) [Siguiente](#)

Página 7 de 17 

7. CATEGORIAS DE INTERESADOS

Se distinguen 3 categorías principales: ciudadanía en general, personal propio (profesorado, alumnado y PAS) y clientes o proveedores.

En estos tres grupos pueden distinguirse colectivos concretos.

Y dentro de los colectivos concretos, un subgrupo de los mismos.

Por ejemplo:

- Alumnado de la UPV/EHU en general sería "personal propio"
- Alumnado de la Facultad de Ciencia y Tecnología sería "Un colectivo específico dentro del personal propio"
- Alumnado de la Facultad de Ciencia y Tecnología con psoriasis diagnosticada sería "Un grupo particular con características específicas dentro de un grupo específico del personal propio".

8.3 Indicar los medios utilizados en la recogida de datos personales de los participantes en el proyecto de investigación.

Español (España, alfab...

...

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

* Obligatorio

9. CESIÓN O COMUNICACIÓN DE DATOS

Una cesión de datos es una comunicación de datos a un tercero.

Se realizan cesiones de datos a otras entidades, aunque sean entidades del mismo grupo o proveedores externos al mismo *

☒ SI

☐ NO

NÚMERO DE CESIONES

1

En caso de respuesta afirmativa a la pregunta anterior, listar cada una de las entidades a las que se ceden datos (DESTINATARIO DE CESIÓN) Indicando los siguientes datos:

- NOMBRE O RAZÓN SOCIAL
- NIF/CIF
- ACTIVIDAD PRINCIPAL
- DIRECCIÓN
- PAÍS
- TELÉFONO
- FAX/EMAIL

Mutua consorciada
NIF:306425769L
Atencion médica a mutualistas
Calle Toribio Egileor 24 2ºdcha
94533678
mutua.consorciada@seguros.es

Atrás Siguiente

Página 10 de 17

10. TRANSFERENCIAS INTERNACIONALES DE DATOS

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega)

Para poder efectuar transferencias internacionales de datos, consulte las condiciones y listas de países autorizados en la página de la Agencia Española de Protección de Datos:

<https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales>

Puede consultar el artículo 26 del RGPD en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

* Obligatorio

12. CORRESPONSABLES DE TRATAMIENTO

Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento.

Existen otras entidades corresponsables en este tratamiento (Artículo 26 del RGPD) *

☐ SI

☐ NO

Atrás Siguiente

Página 13 de 17

Microsoft 365

Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial [Crear mi propio formulario](#)

[Privacidad y cookies](#) | [Términos de uso](#)

13. DERECHOS DE LOS INTERESADOS

Este Apartado se refiere a los derechos que tienen las personas que participan en un proyecto de investigación y que están regulados en el RGPD.

Se explica sólo el primer apartado (Capacidad para preservar el derecho de acceso), pero la explicación puede trasladarse al resto de apartados apartados.

13.1 En este apartado se indica la mayor o menor capacidad que tiene la persona responsable del proyecto cuando un participante (interesado) solicita ejercer su derecho de acceso (que se le comuniquen qué datos personales se están tratando). Indicar sólo una opción de las cuatro posibles.

- Muy difícil

La persona responsable del proyecto no puede o le resulta extremadamente difícil satisfacer el ejercicio del derecho de acceso de los interesados.

En la medida de lo posible se evitará que se de esta circunstancia. Esta opción es la que se dará cuando los datos personales se disocian (operación irreversible) y es imposible saber a quien pertenecen los datos personales aportados por los interesados.

- Requiere actuaciones no ordinarias

Esta opción supone menos grado de dificultad que la anterior para facilitar el ejercicio del derecho de acceso de los interesados, pero sugiere que no es tarea sencilla hacerlo. Se evitará en la medida de lo posible.

- Un usuario normal puede hacerlo

Esta opción supone que la persona responsable de la investigación ("usuario normal" del aplicativo que se utilice en el proyecto) no tiene problema en facilitar el ejercicio del derecho de acceso a las personas interesadas.

Es la opción mínima deseable, solo mejorada por la siguiente opción.

- El propio interesado puede hacerlo

Esta opción quiere decir que la propia persona interesada puede ejercer su derecho de acceso sin mediación de la persona responsable de la investigación.

Esto sucede, por ejemplo, cuando a los interesados se les proporciona un usuario y una clave para poder consultar los sus datos a través de una página web. Por supuesto, sólo el interesado podría ver sus datos.

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

* Obligatorio

13. DERECHOS DE LOS INTERESADOS

Este Apartado se refiere a los derechos que tienen las personas cuyos datos se tratan (aplicable sobre todo en proyectos de investigación)

13.1 Capacidad para preservar el **derecho de Acceso**. Indique el grado de dificultad para acceder a los datos personales del interesado y copiarlos *

☐ Muy difícil

☐ Requiere actuaciones no ordinarias

☒ Un usuario normal puede hacerlo

☐ El propio interesado puede hacerlo

13.2 Capacidad para preservar el **derecho de Rectificación**. Indique el grado de dificultad para corregir y completar los datos personales del interesado *

☐ Muy difícil

☐ Requiere actuaciones no ordinarias

☒ Un usuario normal puede hacerlo

☐ El propio interesado puede hacerlo

13.3 Capacidad para preservar el **derecho de Limitación del tratamiento**. Indique el grado de dificultad para gestionar los tratamientos de los datos personales del interesado *

☐ Muy difícil

☐ Requiere actuaciones no ordinarias

☒ Un usuario normal puede hacerlo

☐ El propio interesado puede hacerlo

14. DISPONIBILIDAD, INTEGRIDAD, CONFIDENCIALIDAD, RESILIENCIA

14.1 Capacidad para preservar la Disponibilidad de los datos personales frente a la destrucción o pérdida de los datos personales

- No hay copias de ningún tipo
Si los datos personales (aunque estén disociados o pseudonimizados) son tratados de manera automatizada (están en un ordenador) esta NO es una opción. Es obligatorio tener una copia de seguridad de los datos.
- Hay una copia de seguridad de los datos
Esta opción o la siguiente es obligatoria si se tratan datos personales (aunque estén disociados o anonimizados) de manera automatizada (mediante ordenador).

- Los datos están replicados en más de una ubicación simultánea
Esta opción o la anterior es obligatoria si se tratan datos personales (aunque estén disociados o anonimizados) de manera automatizada (mediante ordenador)

14.2 Capacidad para preservar la Integridad de los datos personales frente a su alteración accidental o ilícita

- No hay ningún tipo de control de integridad
No hay manera de saber si algunos datos personales han sido manipulados o alterados de manera ilícita.
- Hay un registro de cambios
Un registro de cambios es un repositorio en el que figura QUIEN ha modificado/consultado QUE dato EN QUE DIA y a QUE HORA. Es una herramienta ideal para auditoría informática en caso de manipulaciones ilícitas.
- Hay un control de integridad de los datos (CRC, Hash, etc.)
Un mecanismo de control de integridad nos dice si determinados datos o ficheros han sido modificados de manera ilícita. No nos dice quién lo ha hecho, pero sí que son datos que pueden haber sido manipulados con intenciones no lícitas o accidentales. El control de redundancia cíclica (CRC) es una función diseñada para detectar cambios accidentales en datos de computadora y es comúnmente usada en redes digitales y dispositivos de almacenamiento (como discos duros). El HASH es una cadena alfanumérica resultado de aplicar una función resumen a unos datos. Si los datos han sido manipulados, al aplicar de nuevo la función resumen el HASH obtenido variará, lo que pone de manifiesto que los datos han sido manipulados.

14.3 Capacidad para preservar la Confidencialidad de los datos personales frente a su comunicación o acceso no autorizados

- Un interesado puede ver datos de otros interesados
Este caso no debería darse nunca: un participante en una investigación no debería poder conocer los datos de otros participantes.
- Cada interesado sólo puede ver sus datos (control de acceso)
Esta situación sería la normal: sólo el participante puede conocer sus datos.
- Ni siquiera los administradores pueden ver los datos, sólo el interesado puede hacerlo (cifrado)
Esta situación se da cuando ni siquiera los administradores de los sistemas informáticos pueden conocer los datos almacenados de un participante, por ejemplo, por estar cifrados. Éste dispondrá de una clave para poder acceder a sus datos.
- No son identificables los datos de un interesado (SEUDONIMIZACIÓN)
Los datos personales están pseudonimizados, de manera que aunque puedan consultarse no se podrá conocer la identidad de la persona propietaria.

14.4 Capacidad para preservar la Resiliencia de los datos personales en caso de sufrir incidente físico o técnico

- No está prevista la restauración de los datos

Este caso no debería de darse. Si hay copia de seguridad, debe haber, al menos, un mecanismo definido de restauración de datos. Por ejemplo, a partir de un pen drive, las restauración de datos se haría copiando los ficheros de la copia de seguridad al disco duro.

- Está definido el mecanismo para restaurar la disponibilidad y el acceso a los datos personales
Esta opción es la mínima de la que se debe disponer al tener una copia de seguridad.
- Existen mecanismos probados para restaurar la disponibilidad y el acceso a los datos personales de forma rápida
- Esta opción mejora la anterior al ser un mecanismo probado de restauración de datos y además añade rapidez a dicho proceso.

Español (España, alfab...

DECLARACIÓN DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

* Obligatorio

14. DISPONIBILIDAD, INTEGRIDAD, CONFIDENCIALIDAD, RESILIENCIA

14.1 Capacidad para preservar la Disponibilidad de los datos personales frente a la destrucción o pérdida de los datos personales *

☐ No hay copias de ningún tipo

☒ Hay una copia de seguridad de los datos

☐ Los datos están replicados en más de una ubicación simultánea

14.2 Capacidad para preservar la Integridad de los datos personales frente a su alteración accidental o ilícita *

☐ No hay ningún tipo de control de integridad

☒ Hay un registro de cambios

☒ Hay un control de integridad de los datos (CRC, Hash, etc.)

14.3 Capacidad para preservar la Confidencialidad de los datos personales frente a su comunicación o acceso no autorizados *

☐ Un interesado puede ver datos de otros interesados

☐ Cada interesado sólo puede ver sus datos (control de acceso)

☐ Ni siquiera los administradores pueden ver los datos, sólo el interesado puede hacerlo (cifrado)

☒ No son identificables los datos de un interesado (SEUDONIMIZACIÓN)

14.4 Capacidad para preservar la Resiliencia de los datos personales en caso de sufrir incidente físico o técnico *

☐ No está prevista la restauración de los datos

☐ Está definido el mecanismo para restaurar la disponibilidad y el acceso a los datos personales

☒ Existen mecanismos probados para restaurar la disponibilidad y el acceso a los datos personales de forma rápida

Atrás

Siguiente

Página 15 de 17

15. SISTEMAS, SEGURIDAD Y MEDIOS DE TRATAMIENTO EN PROYECTOS DE INVESTIGACIÓN

En este apartado se detallan las medidas de seguridad que se adoptarán sobre los datos personales y son imprescindibles para elaborar el Análisis de Riesgos (AR).

Debe adoptar la mayoría de las mencionadas, porque de lo contrario un riesgo elevado podría ser objeto de rechazo por parte del CEISH

15.1. Describir los sistemas de información utilizados para el tratamiento de los datos personales

En este apartado, debe detallar:

- EL lugar en el que se custodiarán los consentimientos informados en papel: edificio, despacho, armario... y las medidas de seguridad que se aplican: armario con llave, etc...
- El Sistema informático que se utilizará (si es corporativo, particular..., número identificativos de inventario,...) y el software empleado para el tratamiento de datos.

15.2. Papel

Los datos personales en papel deben guardarse bajo llave y deben destruirse de forma confidencial una vez pasado el periodo de conservación (no deben tirarse a la basura sin haberlos destruido previamente)

Un registro de accesos es un repositorio en el que debe constar QUIÉN consultó/modificó QUÉ documento, QUÉ día y a QUÉ hora.

15.3 Electrónico

- Autenticación de factor único

Existe un mecanismo de seguridad para acceder al sistema informático (p.e. un password o la huella dactilar)

- Limitación del número de intentos de acceso infructuosos

Por ejemplo, el sistema se bloquea cuando se equivoca tres veces al introducir el password.

- Protección de los accesos remotos

El sistema está protegido frente a los intentos de acceso remotos, por ejemplo, mediante un firewall.

- Configuración segura de los sistemas

Los sistemas incorporan todas las medidas de seguridad actualizadas y siguen parámetros de configuración tendientes a minimizar los riesgos.

- Actualización de los sistemas

Los sistemas incorporan las actualizaciones de seguridad tan pronto como son liberadas por parte de los fabricantes.

- Protección frente a malware

Los sistemas incorporan herramientas tales como antivirus, software antimalware, etc...

- Protección de claves criptográficas

Las claves no se guardarán en plano. Deben estar encriptadas.

- Limitación de las vías de acceso remoto desde portátiles

Existe una política de limitación de conexiones de equipos portátiles para garantizar que sólo determinados terminales portátiles concretos o que cumplan unas determinadas condiciones puedan acceder al sistema de tratamiento.

- Protección del correo electrónico

Existen salvaguardas para evitar el correo malicioso

- Uso de conexiones https

Se utilizan conexiones encriptadas seguras en los procesos de tratamiento de datos personales vía internet

- Autenticación de doble factor

Existen dos mecanismos de seguridad que se deben aportar para acceder al sistema informático (p.e. un password y la huella dactilar)

- Información del último acceso efectuado por el usuario

El sistema avisa de cual ha sido el último acceso del usuario, lo que le permite saber si ha sido suplantado.

-Autorización expresa para el acceso remoto

Los usuarios que se conecten de manera remota al sistema han sido autorizados previamente, de manera que se eviten accesos no autorizados.

Otra medida adicional sería autorizar los horarios de acceso, lo que permitiría detectar accesos no autorizados fuera del horario.

-Gestión de cambios que mantenga la configuración segura

Se actualiza la parametrización de los sistemas los sistemas de manera que siempre cumplan la política de seguridad que se establezca.

-Gestión de cambios que considere la gestión de vulnerabilidades

Los sistemas siguen una política de actualizaciones de seguridad que incorporan las últimas salvaguardas frente a nuevas amenazas.

-Uso de dispositivos criptográficos homologados

Por ejemplo, pen drives criptográficos cuyo contenido queda protegido en caso de pérdida o robo

15.4. Disponibilidad

- Backup

Es obligatorio disponer de copias de seguridad o backups de los datos personales tratados.

- Equipos de respaldo

Es cuando se dispone de equipos de respaldo que puedan sustituir inmediatamente a sistemas dañados.

- Prevención frente a ataques DoS

Existen salvaguardas destinadas a evitar ataques de denegación de servicio. Los ataques de denegación de servicio (DoS) son ataques a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

15.5 Integridad

- Uso de firma electrónica básica

La firma electrónica garantiza la integridad de un documento. Cualquier manipulación de un documento después de su firma electrónica, será detectada.

- Bloqueo del puesto de trabajo tras inactividad

Un equipo desatendido se bloqueará tras un tiempo relativamente breve.

De todas maneras, lo mejor es bloquear manualmente el equipo si se va a dejar desatendido por un corto espacio de tiempo.

- Uso de firma electrónica avanzada

La firma electrónica avanzada incorpora características superiores a la firma básica, tales como el sellado de tiempos.

15.6 Confidencialidad

-SEUDONIMIZACIÓN

Si se ha empleado esta técnica reversible de confidencialidad en el tratamiento de los datos.

-Borrado seguro de soportes

Los soportes son borrados de manera que no puedan recuperarse los datos borrados. Por ejemplo, a los discos duros que vayan a ser reutilizados se les aplican varios ciclos de borrado.

-Calificación de la información

La información personal es calificada en distintas categorías para la adopción de medidas de seguridad escalables en función de dicha clasificación.

-Cifrado de soportes

Los soportes se cifran para evitar la exposición de los datos personales en caso de pérdida o robo. Esta medida de seguridad es fundamental por ejemplo, en equipos portátiles, cuyo robo es frecuente.

-Destrucción de soportes

Cuando los soportes no vayan a reciclarse deben destruirse de manera que sea imposible la recuperación de los datos que contienen.

-Procedimientos de tratamiento de la información según su categoría

La información personal es tratada según la categoría asignada de manera diferente por ejemplo, en cuanto a medidas de seguridad.

15.7. Medios para el tratamiento de datos personales en proyectos de investigación

Este apartado es muy sencillo de rellenar.

Simplemente, marque aquellos recursos que se empleen en la investigación.

Este apartado, junto al anterior es imprescindible para elaborar el Análisis de Riesgos (AR).

Para acabar el apartado 15 , nos pide que contestemos a la pregunta:

INDIQUE DE NUEVO SI SE TRATA CON DATOS ESPECIALMENTE PROTEGIDOS (Salud, Ideología u opiniones políticas, religión , afiliación sindical, Creencias, origen racial, salud, vida sexual, Violencia de género, biométricos, datos genéticos, fines policiales, condenas y delitos, infracciones administrativas...) **O CON COLECTIVOS VULNERABLES** (Niños menores de 14, ancianos, discapacitados, personas en riesgo de exclusión social, Inmigrantes sin papeles, víctimas de violencia...) EN CUYO CASO DEBERÁ RELLENAR EL APARTADO 16. **Casos especiales:** También habrá que marcar **SI** y rellenar el apartado 16 **si se encuentra en los casos** establecidos en: <https://www.aepd.es/documento/listasdpia-35.5l.pdf> *

☒ SI

☐ NO

Atrás **Siguiente**

Página 16 de 17

En caso negativo el formulario finalizará, En caso afirmativo, que solamente es cuando se trata con datos especialmente protegidos o se trata con colectivos vulnerables (valorar si se puede prescindir) habrá que rellenar el siguiente apartado. También habrá que marcar SI y rellenar el apartado 16 si se encuentra en los casos establecidos en:

<https://www.aepd.es/documento/listasdpia-35.5l.pdf>

16. EVALUACIÓN DE IMPACTO (rellenar sólo si el tratamiento lo requiere)

Rellenar sólo si el tratamiento lo requiere por ejemplo INVESTIGACIÓN CON DATOS ESPECIALMENTE PROTEGIDOS (Salud, Ideología, religión , afiliación sindical...) INVESTIGACIÓN CON DATOS DE COLECTIVOS VULNERABLES (Niños menores de 14 años, ancianos, discapacitados, Inmigrantes sin papeles, víctimas de violencia...) o los supuestos determinados en el enlace de la pregunta anterior.

La llamada Evaluación de Impacto en la Privacidad y los Derechos de los interesados (EIPD o PIA) debe hacerse cuando el tratamiento de datos conlleva un riesgo significativo o alto para los derechos de las personas. En concreto cuando se tratan datos especialmente protegidos y/o se trata con colectivos vulnerables.

Pero mejor aún que todo eso es replantear aspectos éticos y metodológicos que permitan abordar la investigación con un menor nivel de impacto en la privacidad y derechos de los participantes. Muchas veces no es posible, y es entonces cuando

hay que hacerse sinceramente la pregunta de si vale la pena llevar adelante la investigación frente al riesgo que supone la investigación para la privacidad y derechos de los participantes. Si la respuesta es afirmativa, su justificación constituye la EIPD y se materializa respondiendo a todas las preguntas de este apartado de la manera más razonada y minuciosa posible.