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

Contenido

Inicio 2

1. Responsable del tratamiento 4

2. NOMBRE DEL TRATAMIENTO 5

3. FINALIDAD DEL TRATAMIENTO DE DATOS 6

4. LEGITIMACIÓN DEL TRATAMIENTO 11

5. ESTRUCTURA BÁSICA Y DESCRIPCIÓN DE LOS TIPOS DE DATOS DE CARÁCTER PERSONAL INCLUIDOS 12

6. FINALIDAD Y CARACTERÍSTICAS DEL TRATAMIENTO 14

7. CATEGORIAS DE INTERESADOS 16

8. PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA DE LOS DATOS 17

9. CESIÓN O COMUNICACIÓN DE DATOS 18

10. TRANSFERENCIAS INTERNACIONALES DE DATOS 19

11. ENCARGADOS DE TRATAMIENTO 20

12. CORRESPONSABLES DE TRATAMIENTO 20

13. DERECHOS DE LOS INTERESADOS 21

14. DISPONIBILIDAD, INTEGRIDAD, CONFIDENCIALIDAD, RESILIENCIA 22

14.1 Capacidad para preservar la Disponibilidad de los datos personales frente a la destrucción o pérdida de los datos personales 22

14.2 Capacidad para preservar la Integridad de los datos personales frente a su alteración accidental o ilícita 23

14.3 Capacidad para preservar la Confidencialidad de los datos personales frente a su comunicación o acceso no autorizados 23

14.4 Capacidad para preservar la Resiliencia de los datos personales en caso de sufrir incidente físico o técnico 23

15. SISTEMAS,SEGURIDAD Y MEDIOS DE TRATAMIENTO EN PROYECTOS DE INVESTIGACIÓN . 25

15.1. Describir los sistemas de información utilizados para el tratamiento de los datos personales 25

15.2. Papel 25

15.3 Electrónico 25

15.4. Disponibilidad 26

15.5 Integridad 26

15.6 Confidencialidad 26

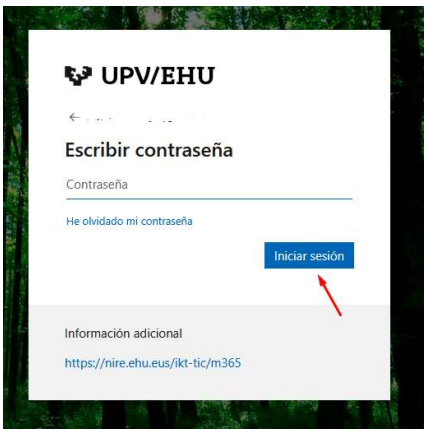
15.7. Medios para el tratamiento de datos personales en proyectos de investigación 27

16. EVALUACIÓN DE IMPACTO (rellenar sólo si el tratamiento lo requiere) 27
16.1. Análisis de las características del tratamiento 28
16.2. Análisis de la necesidad y proporcionalidad del tratamiento 28
16.3. Análisis de los riesgos 30
16.4. Análisis de las medidas de seguridad 30
16.5. Valoración Final 31

Inicio

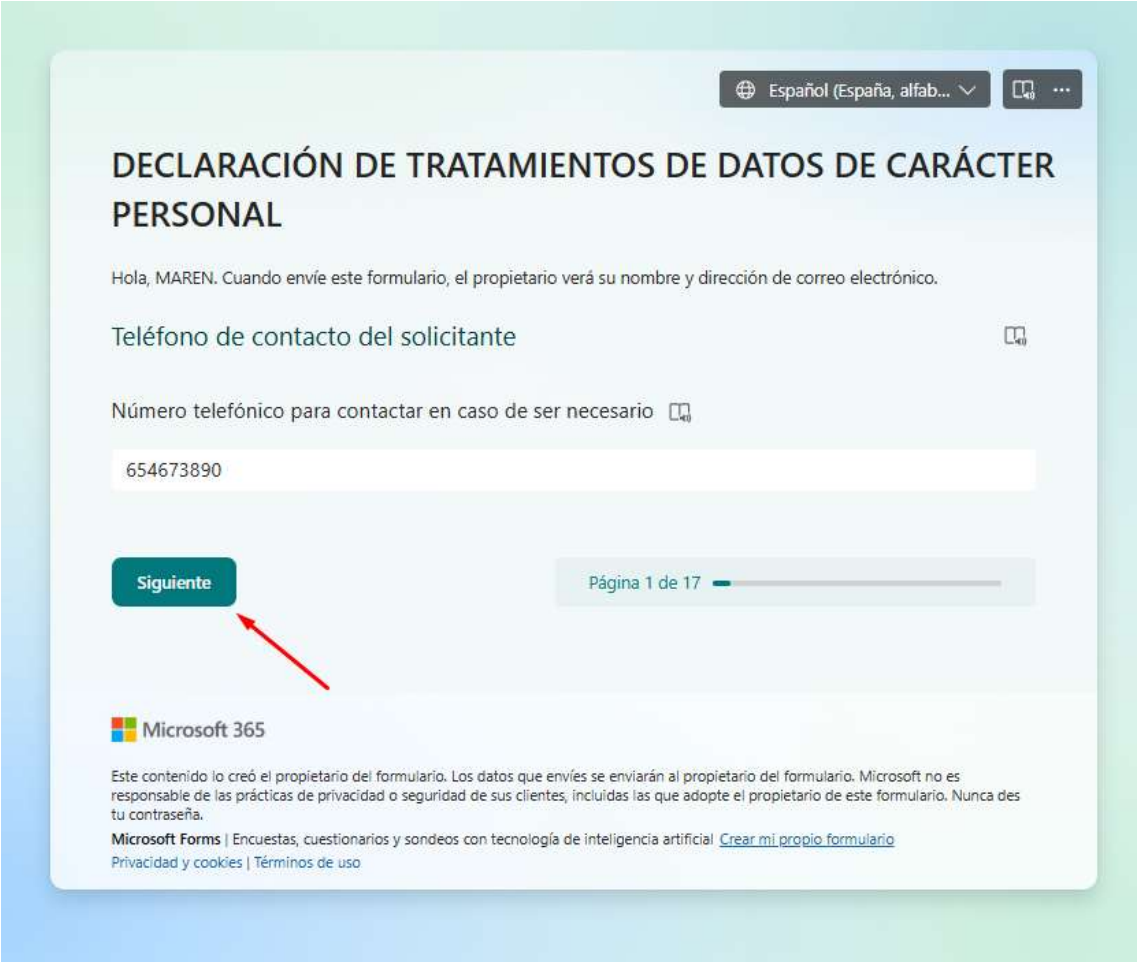
Accedemos a la **siguiente** url: Accedemos al formulario en la url:
https://forms.office.com/e/qcvjTuk901

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



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

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”:



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.

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

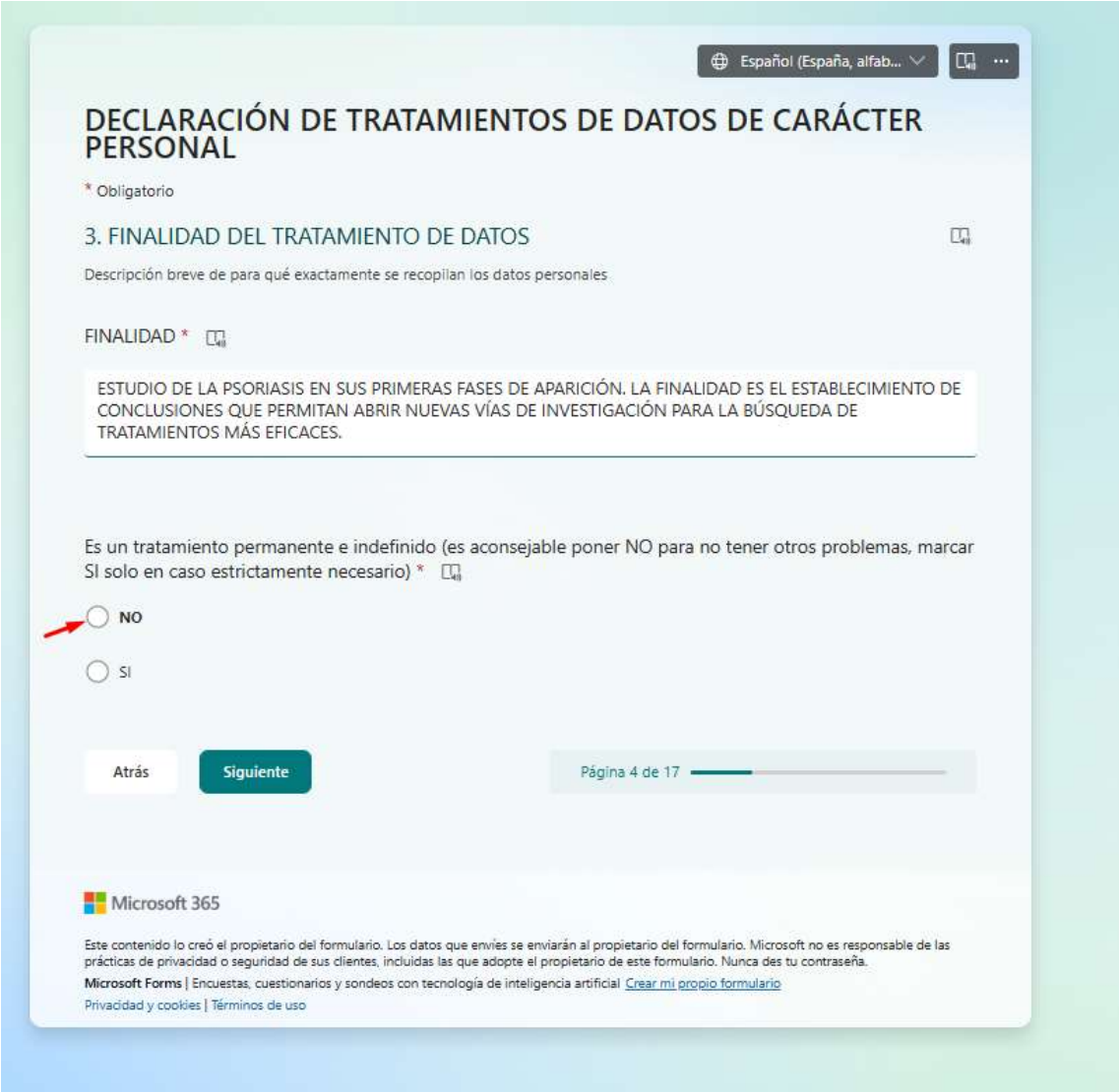
2. NOMBRE DEL TRATAMIENTO

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:

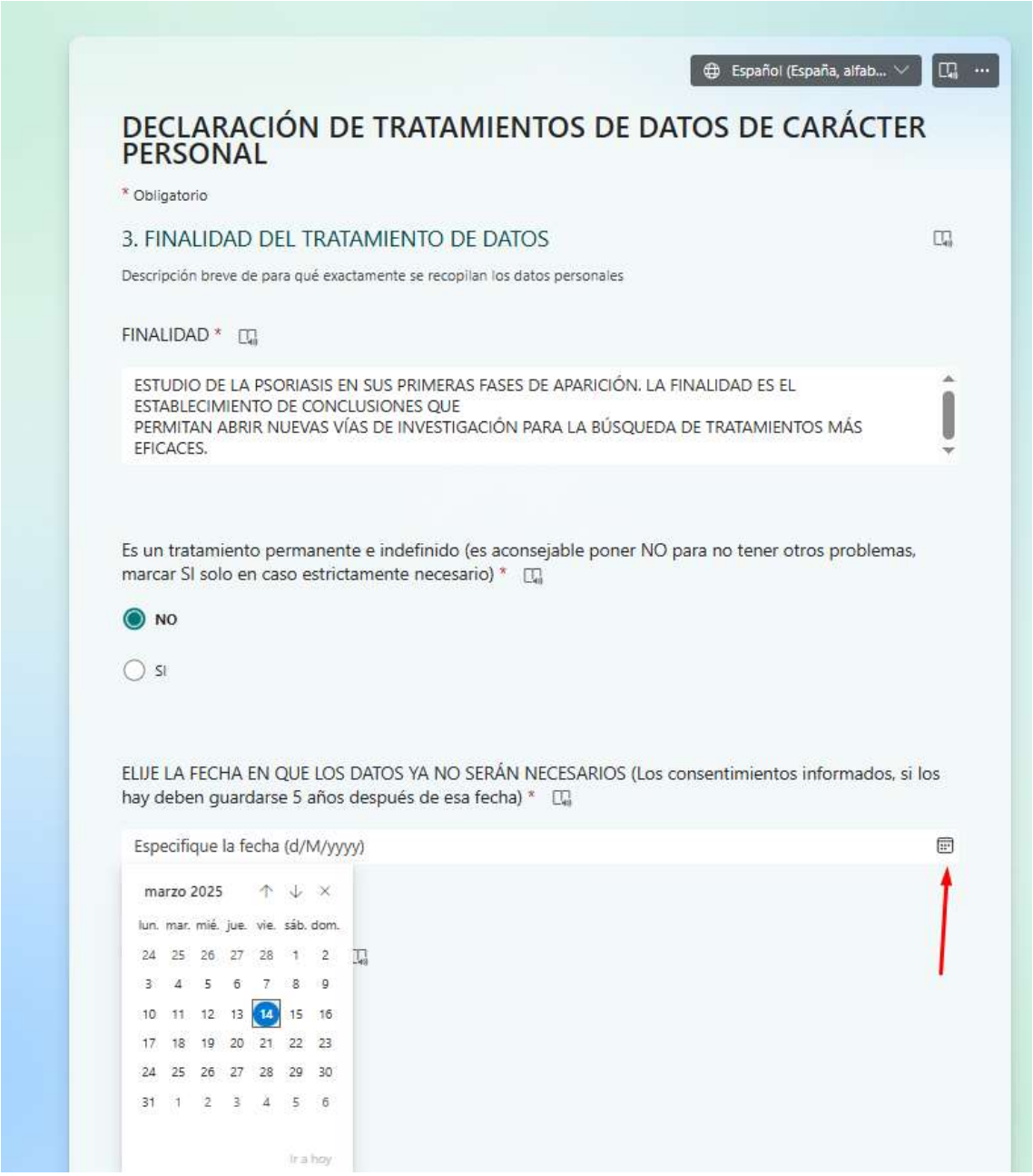
En todo momento **puede ir hacia atrás**, incluso, dependiendo del tipo de navegador **los datos** ya rellenados en el formulario, **no se perderán** aunque reinicie el ordenador.

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..."

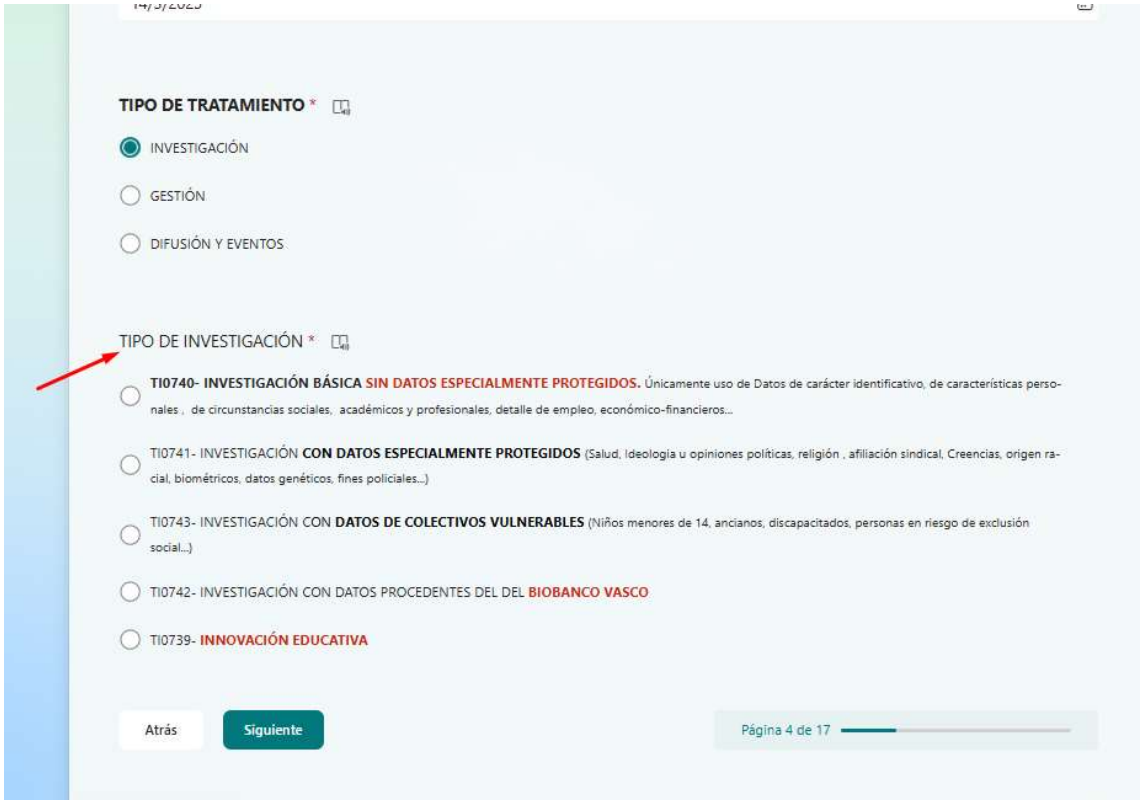


Como se señala con la flecha, es conveniente establecer una fecha de fin de uso de los datos, si no se pueden poner pegas a nivel de delegado de protección de datos, así que solo se debe marcar SI en caso estrictamente necesarios.

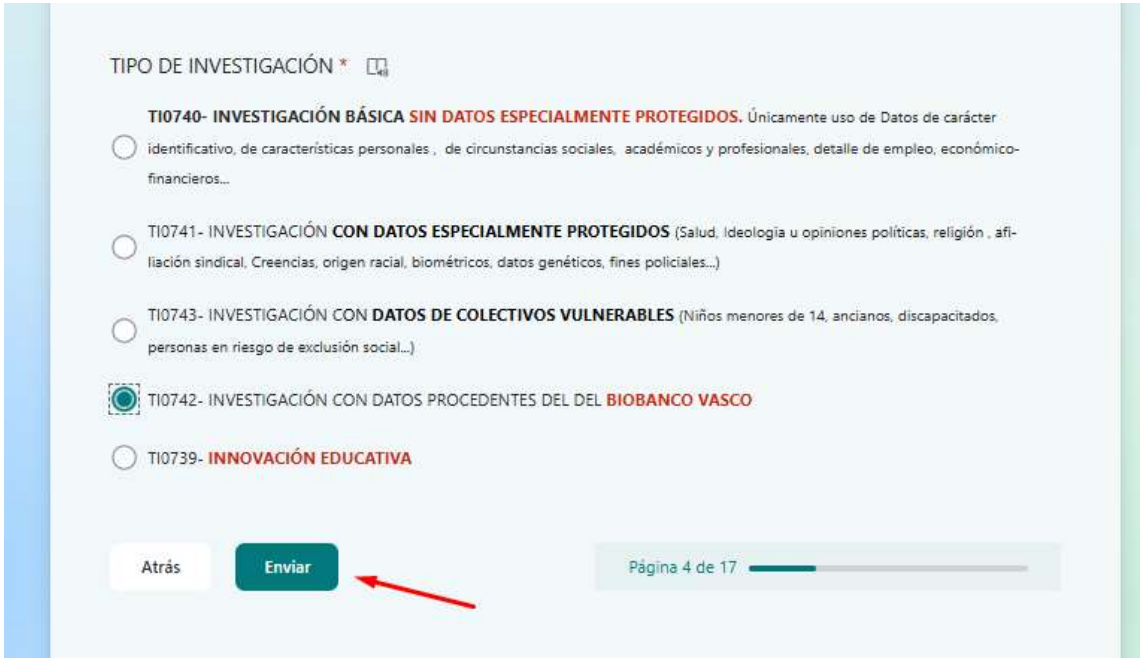


A continuación nos pide el tipo de tratamiento de datos: **Gestión** es para cuestiones administrativas y de gestión, **Investigación** es para proyectos de investigación (Incluyendo innovación educativa) y **difusión y eventos** es para eventos y difusión en general (congresos, difusión en redes sociales…).

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



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



Enel resto de los casos seguimos adelante.

Y nos pide que seleccionemos

EXTENSION GEOGRAFICA DEL TRATAMIENTO (Ámbito territorial del proyecto)

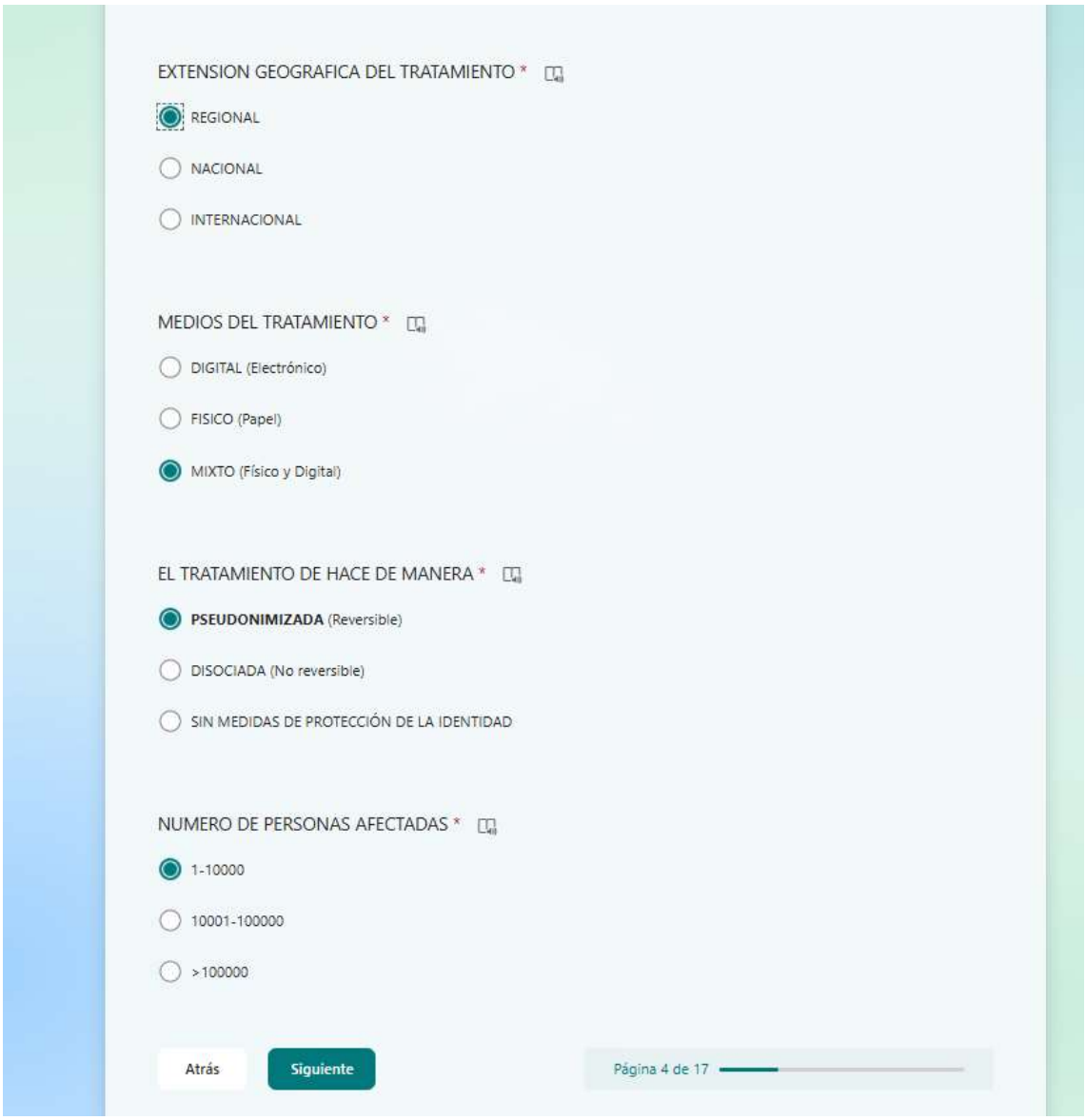
MEDIOS DEL TRATAMIENTO: Aquí se presentan tres opciones: físicos (papel, grabaciones analógicas, fotografías no digitales...), digitales (grabaciones digitales, ficheros informáticos...)

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



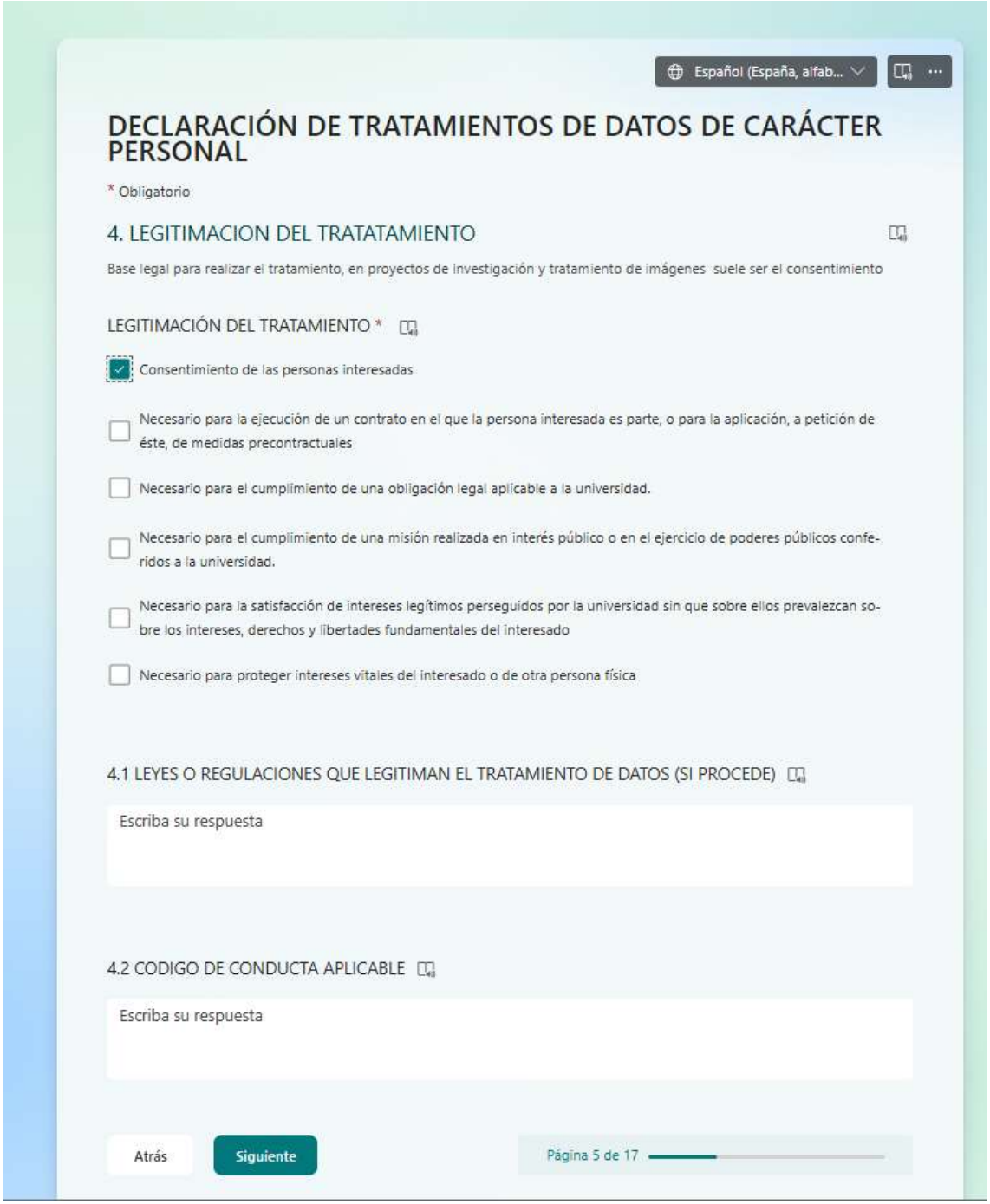
Rellenamos la siguiente sección:

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 cual son la 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.**

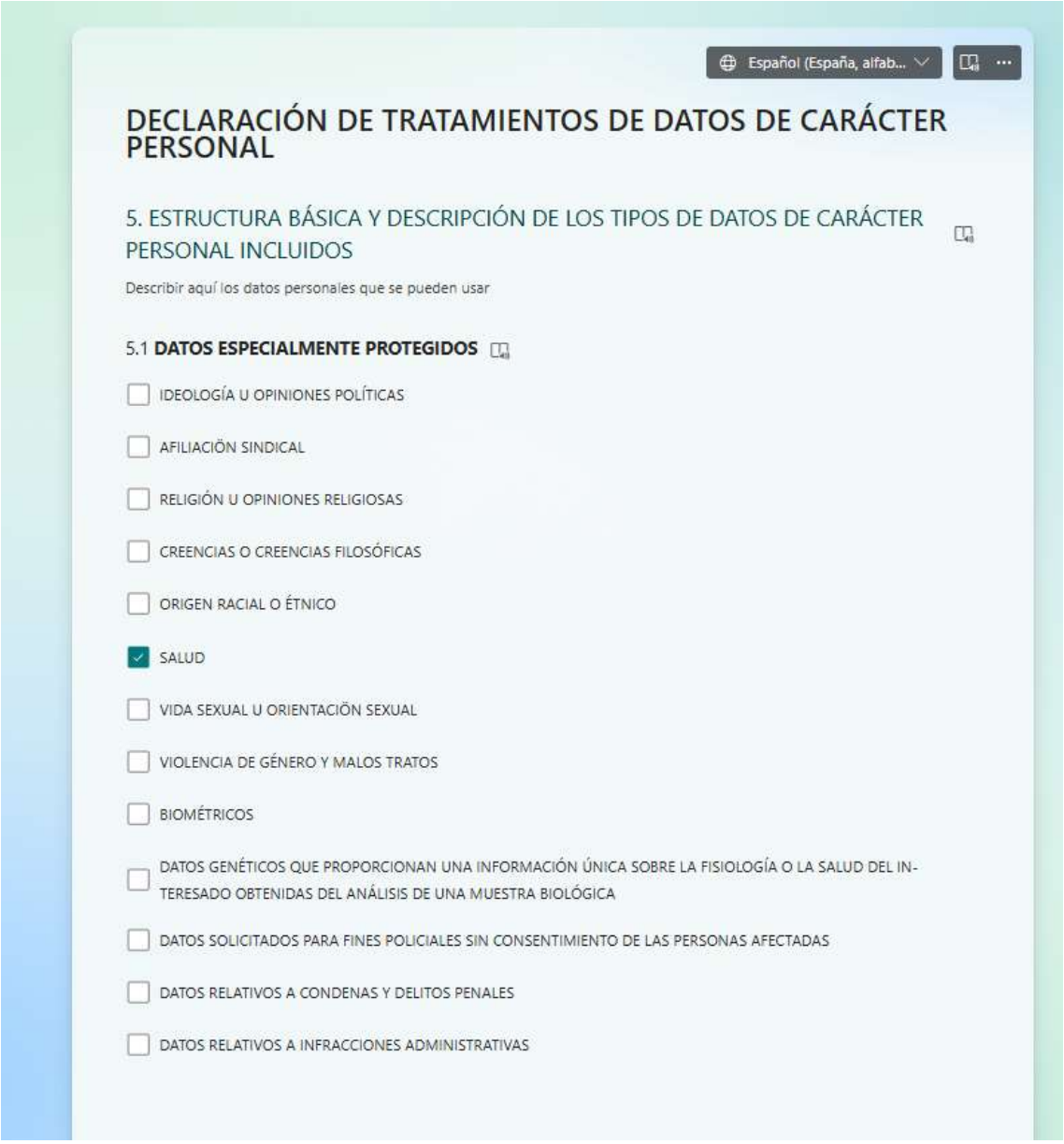
4.2 No rellenar este apartado. De momento la UPV/EHU no ha elaborado ningún código de conducta ni se ha adherido a ninguno existente.



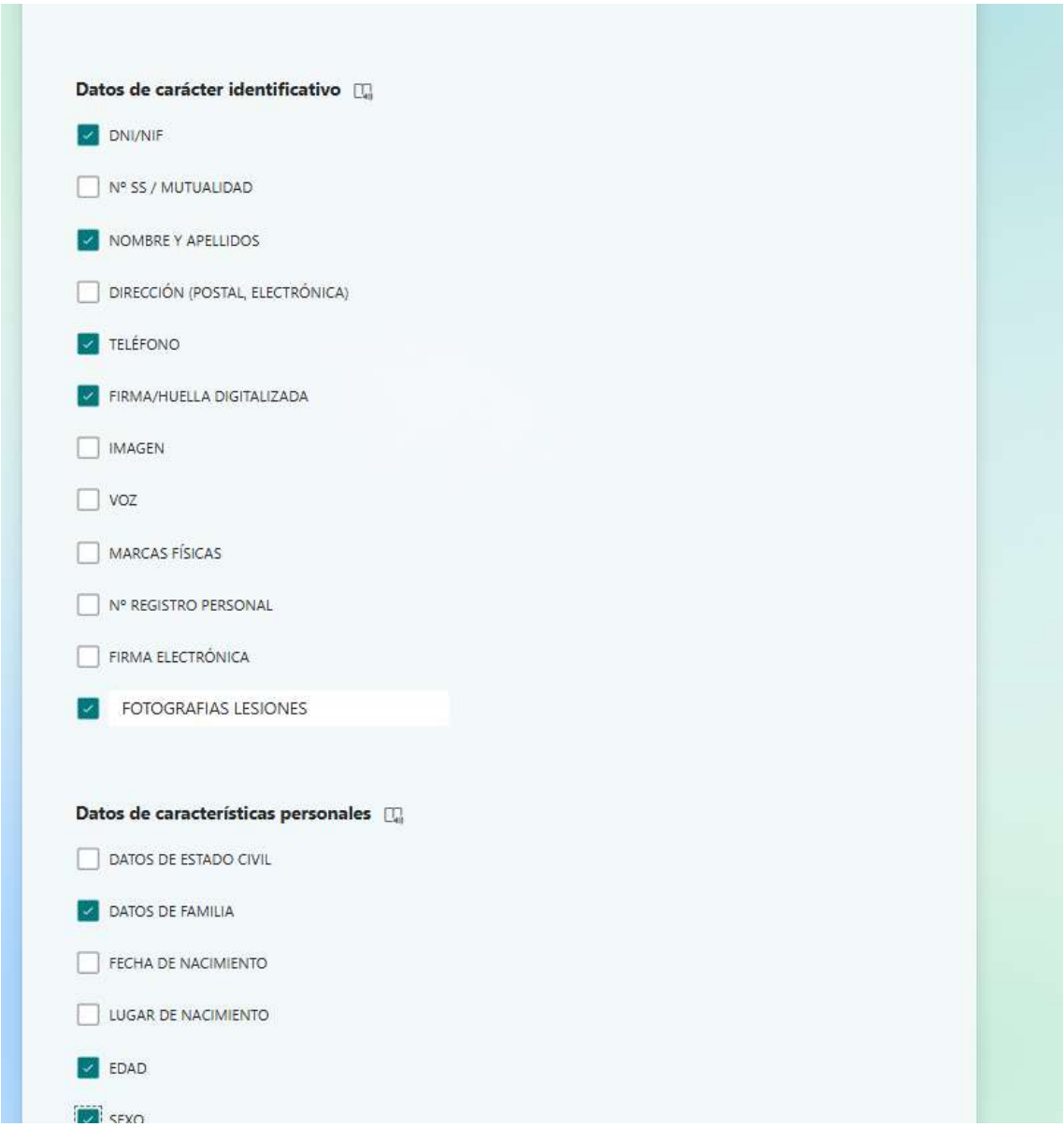
5. ESTRUCTURA BÁSICA Y DESCRIPCIÓN DE LOS TIPOS DE DATOS DE CARÁCTER PERSONAL INCLUIDOS

Describir aquí los datos personales que se pueden usar

Marque todas aquellas categorías de datos que vayan a recabarse, **tanto las afirmativas** (personas con psoriasis implica datos de salud) **como las negativas** (no tener psoriasis es también un dato relativo a la salud).

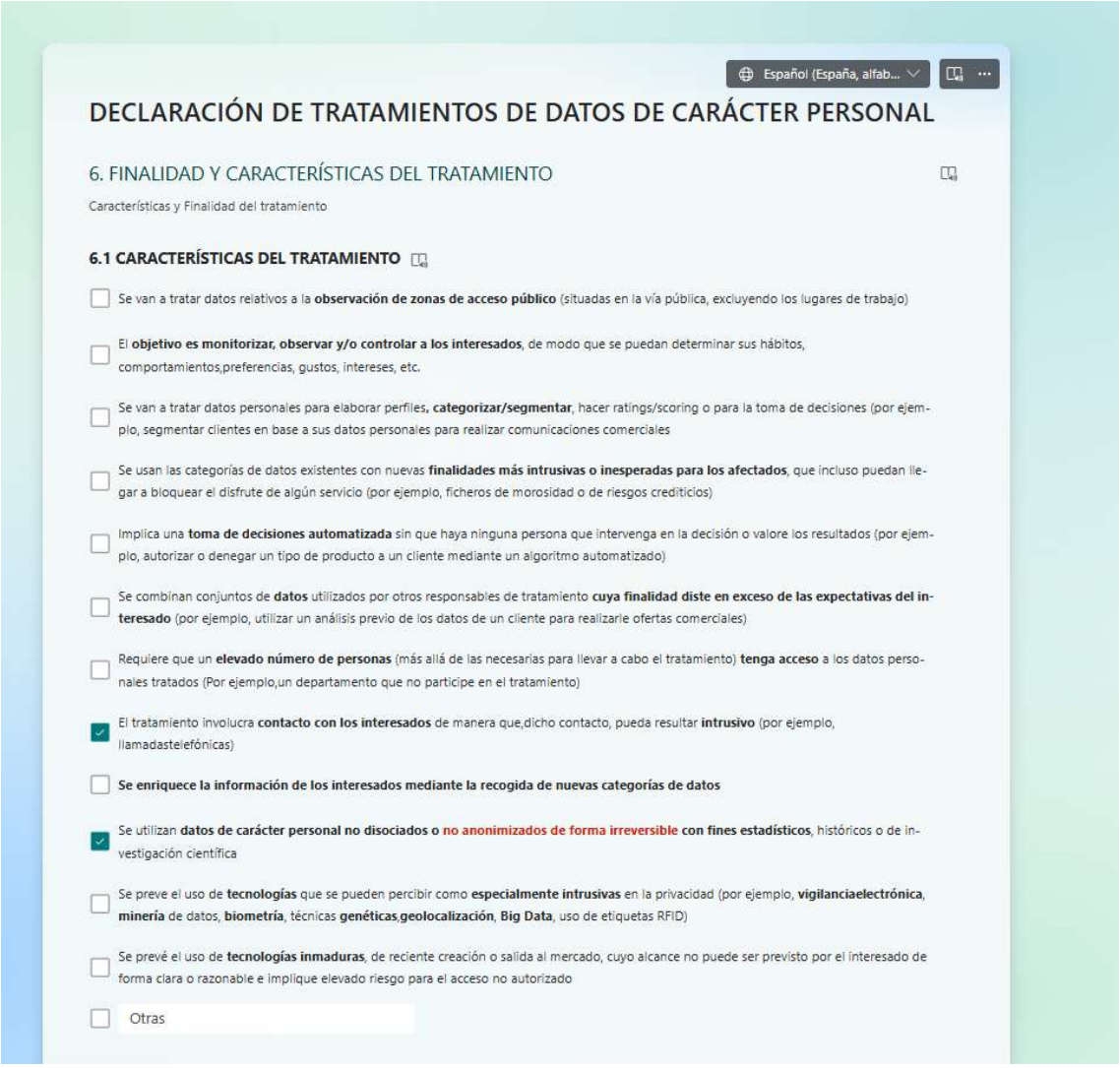


Marque en este apartado cuantos datos vaya a recabar. Si no aparecen en la lista, utilice el campo otros, como en este ejemplo. No olvide marcar, **si recaba consentimientos informados, al menos "NOMBRE Y APELLIDOS" y "FIRMA/FIRMA DIGITALIZADA"**



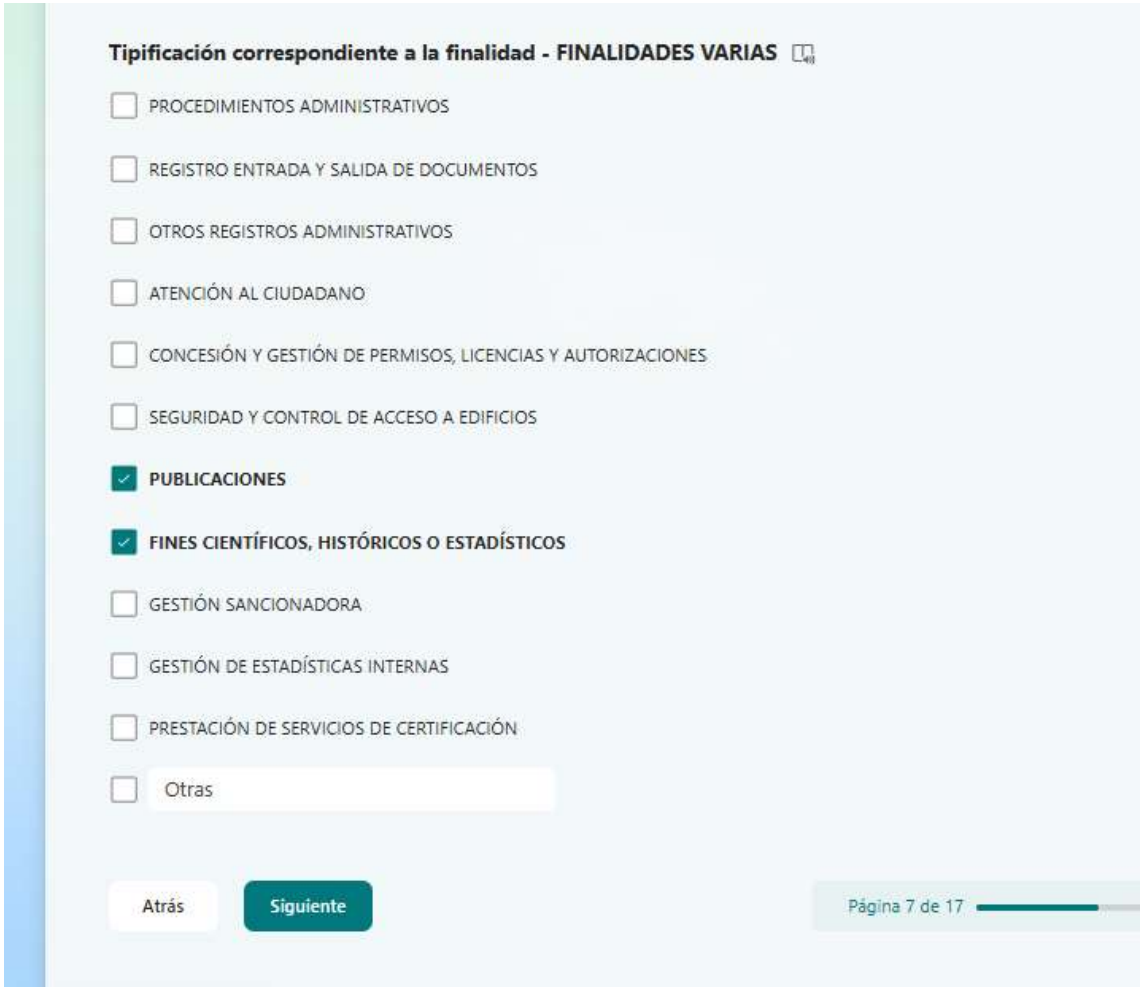
6. FINALIDAD Y CARACTERÍSTICAS DEL TRATAMIENTO

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



Tipificación correspondiente a la finalidad

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.



7. CATEGORIAS DE INTERESADOS

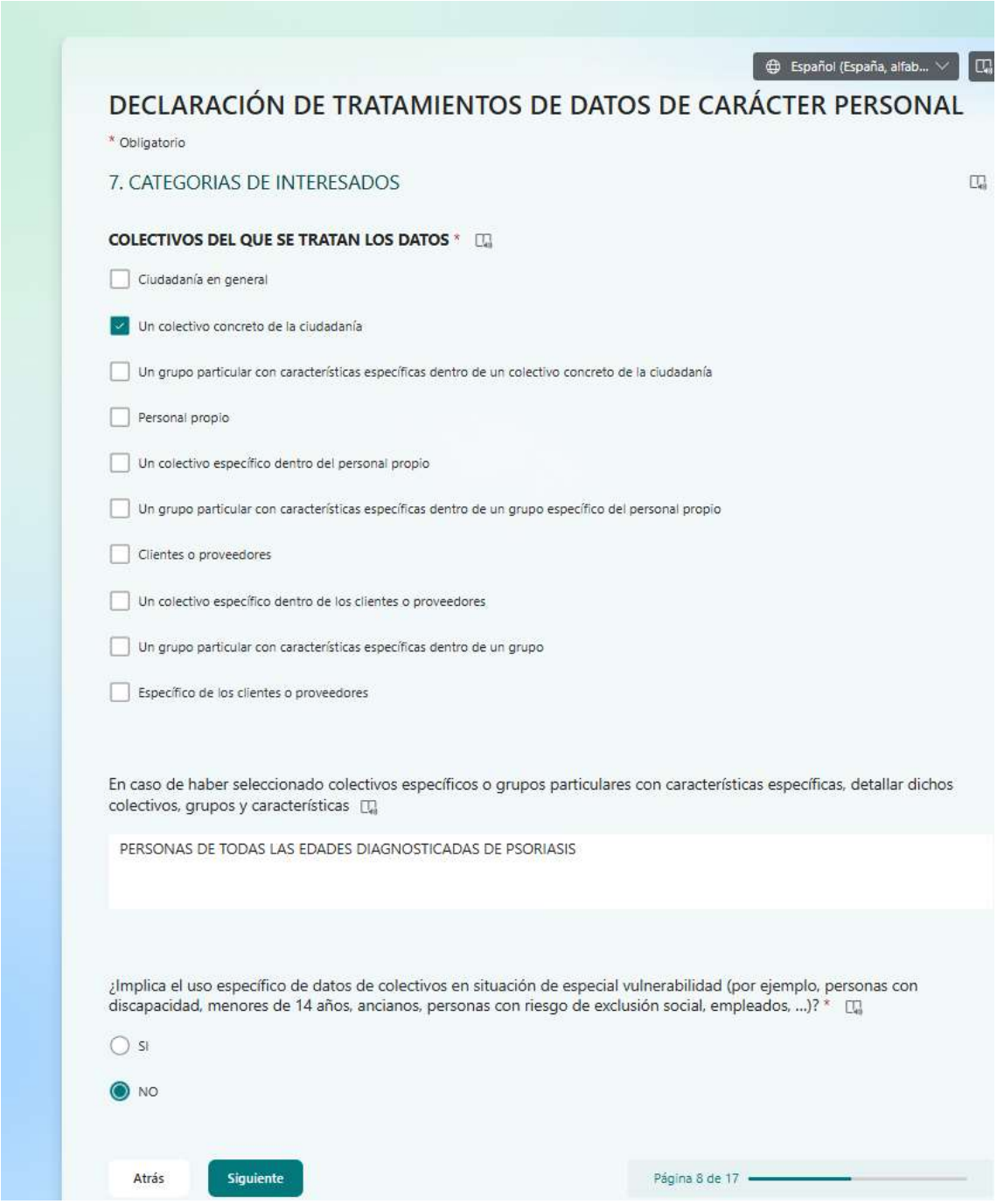
Se distinguen 3 categorías principales: ciudadanía en general, personal propio (profesorado, alumnado y PAS) y clientes o proveedores.

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".



En caso de haber seleccionado un colectivo Describir el colectivo del que se pretenden recabar datos personales.

La ultima opción es obligatoria.

8. PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA DE LOS DATOS

8.1 Indicar la procedencia de los datos personales de los participantes en el proyecto de investigación.
8.2 Indicar como se recogen datos personales de los participantes en el proyecto de investigación.
8.3 Indicar los medios utilizados en la recogida de datos personales de los participantes en el proyecto de investigación.

9. CESIÓN O COMUNICACIÓN DE DATOS

Una cesión de datos es una comunicación de datos a un tercero para que este los aplique a una finalidad para la que no fueron recabados.

Para que una cesión sea lícita debe darse alguna de las siguientes circunstancias:

- Que cuente con el consentimiento previo, específico e inequívoco de los titulares de dichos datos.
- Que la cesión sea necesaria para la ejecución o desarrollo de una relación contractual.
- Que constituya una obligación legal para el cedente.
- Que obedezca a intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.
- Que sirva para salvaguardar el interés vital del interesado o de otras personas.

No se considera cesión de datos la comunicación de los mismos a un encargado de tratamiento. La realización de una prestación de servicios con acceso a datos requiere la existencia de un contrato escrito que establezca expresamente las obligaciones del encargado del tratamiento.

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 paises 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

11. ENCARGADOS DE TRATAMIENTO

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

Si el proyecto de investigación encarga tratamientos de datos a terceros, debe formalizar un contrato o convenio con el mismo donde se mencionen las condiciones del tratamiento.

La UPV/EHU tiene aprobado un modelo de contrato, convenio o acto jurídico que se formalice con los encargados de tratamiento. Puede consultarse en:
https://www.ehu.eus/es/web/idazkaritza-nagusia/2019ko-otsailaren-27ko-erabakia

12. CORRESPONSABLES DE TRATAMIENTO

Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD.

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

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.

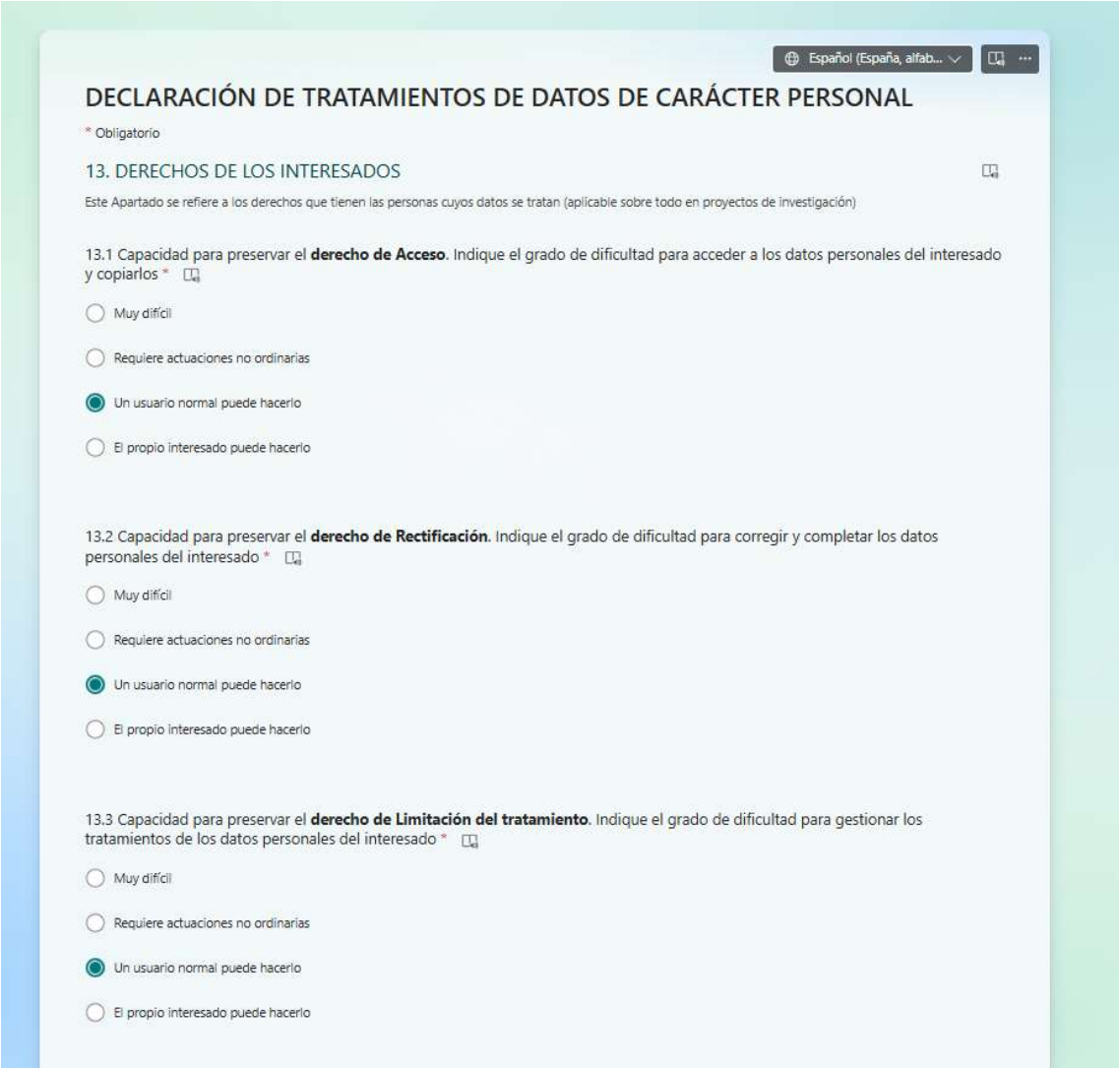
En la medida de lo posible se evitará que se de esta circunstancia. Esta opción es la que se dará cuando los datos personales de disocian (operación irreversible) y es imposible saber a quien pertenecen los datos personales aportados por los interesados.

- 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.



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 auditaría 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.

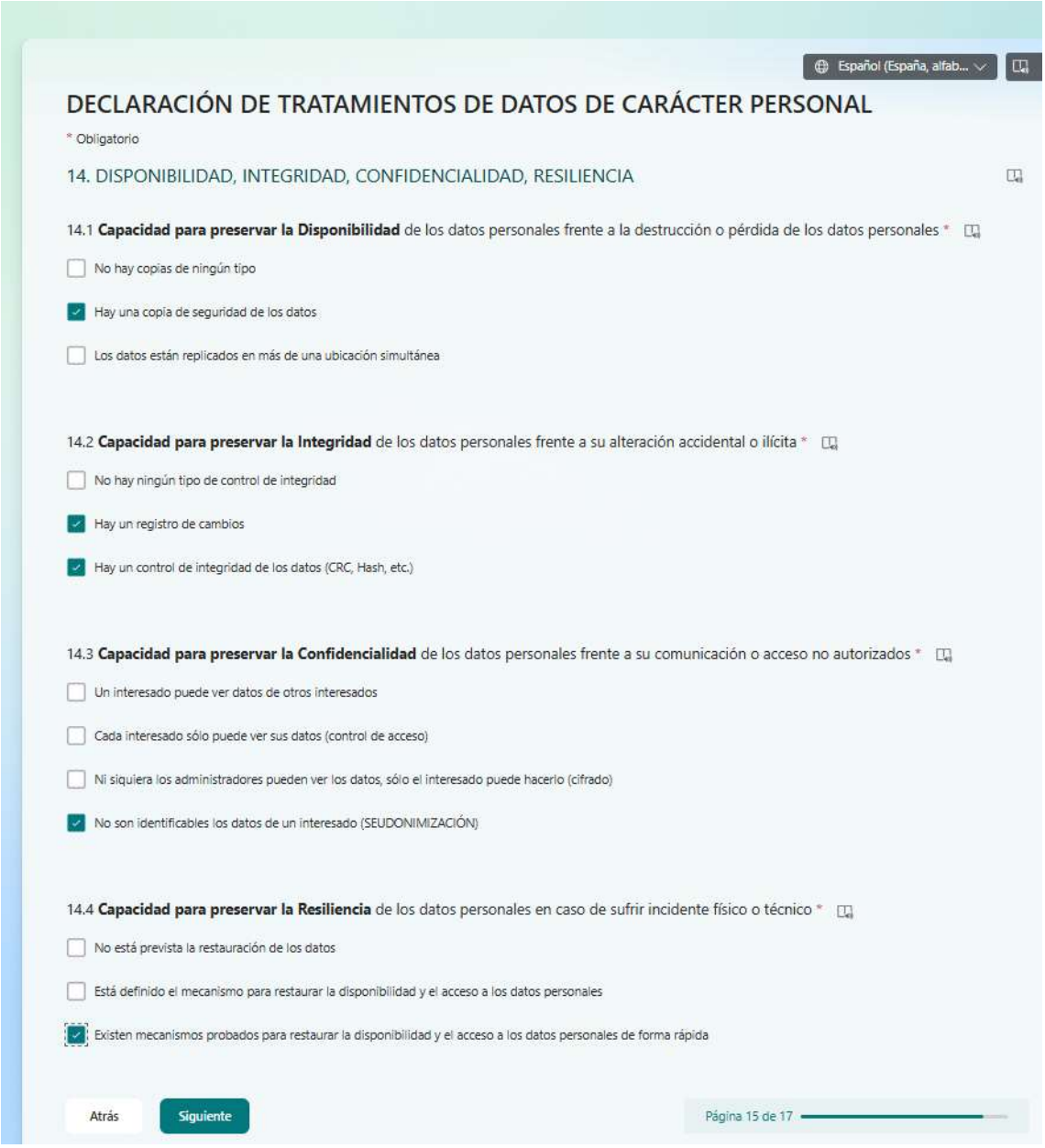
14.4 Capacidad para preservar la Resiliencia de los datos personales en caso de sufrir incidente físico o técnico

- 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.



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 si 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 en 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 tendentes 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 guaradarán en plano. Deben estar encriptadas.
- Limitación de las vías de acceso remoto desde portátiles
Existe un 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 sqguen un 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 sitemas dañados.
- Prevención frente a ataques DoS
Esisten salvaguardas destinadas a evitar ataque 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 brloqueará 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 característica superiores a la firma básica, tales como el sellado de tiempos.

15.6 Confidencialidad

-SEUDONIMIZACIÓN
Si se ha empleado esta técnica revesrible 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:

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, Ideologia, religión , afiliación sindical...) INVESTIGACIÓN CON DATOS DE COLECTIVOS VULNERABLES (Niños menores de 14 años, ancianos, discapacitados, Inmigrantes sin papeles, victimas 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.

16.1. Análisis de las características del tratamiento

Analice los apartados 3 a 8 del presente formulario y realice su valoración parcial: ¿El tratamiento de datos personales que se va a llevar a cabo es correcto desde el punto de vista de la finalidad declarada?

SI/NO: Marca **SI** si todas las actividades y datos están alineados con la finalidad declarada sin usos adicionales; marca **NO** si existe alguna desviación o finalidad no informada.
Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Explique por qué las actividades y los datos son necesarios para lograr la finalidad y cómo se garantiza que no se usarán para otros fines.

Ejemplo de respuesta:
El uso de entrevistas, grupos focales y dibujos es imprescindible para obtener información cualitativa directamente relacionada con los objetivos de la investigación; estas técnicas se ajustan a la finalidad declarada y permiten recoger únicamente los datos necesarios, sin usos adicionales no informados (principio de limitación de la finalidad y responsabilidad proactiva).

16.2. Análisis de la necesidad y proporcionalidad del tratamiento

- *Los datos recogidos se van a usar exclusivamente para la finalidad declarada y no van a ser usados para ninguna otra no informada ni incompatible con la legitimidad de su uso (principio de limitación de la finalidad)*

SI/NO: Marca **SI** si se garantiza el uso exclusivo para la finalidad informada; marca **NO** si puede haber un uso diferente o no comunicado.
Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Explique cómo se asegura la ausencia de desvíos de finalidad y qué controles existen para limitar el uso a lo declarado.

Ejemplo de respuesta:

Los datos se utilizarán exclusivamente para la finalidad informada y no se emplearán para fines distintos ni incompatibles; el tratamiento se limita al alcance declarado y se impide cualquier reutilización no prevista, en línea con el principio de limitación de la finalidad y con la responsabilidad proactiva exigida por el RGPD.

- *La finalidad que se pretende cubrir requiere de todos los datos a recabar y que sean recabados para todas las personas/interesados afectados (principio de minimización de datos)*

  SI/NO: Marca **SI** si todos los datos solicitados son indispensables; marca **NO** si alguno no es estrictamente necesario.
  Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Justifique por qué cada dato es imprescindible y confirme que no se recogen datos que no aportan valor.

  Ejemplo de respuesta:

  Cada categoría de datos solicitada es estrictamente necesaria y contribuye de forma directa a los objetivos del proyecto; se ha verificado que no se recaban datos superfluos, cumpliendo el principio de minimización.

- *Las tecnologías empleadas para el tratamiento son adecuadas para la finalidad establecida desde el punto de vista del cumplimiento de los principios fundamentales de la privacidad*

  SI/NO: Marca **SI** si las tecnologías aplican medidas de seguridad adecuadas (cifrado, control de acceso, privacidad por defecto); marca **NO** si no son suficientes.
  Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Explique cómo las tecnologías garantizan confidencialidad, integridad, disponibilidad y cumplimiento del RGP

  Ejemplo de respuesta:

  Las tecnologías utilizadas incorporan cifrado, control de acceso y opciones de anonimización, están alineadas con la política corporativa y permiten aplicar privacidad desde el diseño y por defecto, garantizando confidencialidad, integridad y disponibilidad conforme al RGPD.

- *Los datos se mantienen exclusivamente el tiempo del necesario para las finalidades del tratamiento, y no más (principio de limitación del plazo de conservación:*

  SI/NO: Marca **SI** si existe un plazo definido o criterios claros de conservación y borrado; marca **NO** si no están definidos o son excesivos.
  Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Indique el plazo o criterio de conservación y cómo se eliminarán o anonimizarán los datos al finalizar.

  Ejemplo de respuesta:

  Los datos se conservarán únicamente durante el tiempo necesario para cumplir la finalidad del proyecto y hasta la finalización del análisis y difusión de resultados; a su término se eliminarán o anonimizarán de manera segura, conforme al principio de limitación del plazo de conservación.

- *El tratamiento de datos personales que se va a llevar a cabo es necesario y proporcionado*

SI/NO: Marca **SI** cuando es la opción menos intrusiva posible y los datos son los mínimos necesarios; marca **NO** si existe una alternativa menos invasiva.
Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Explique por qué este tratamiento concreto es necesario y cómo se ajusta al principio de proporcionalidad.

Ejemplo de respuesta:

El tratamiento es necesario y proporcionado porque no existe una alternativa menos intrusiva que ofrezca resultados equivalentes, y se limita a los datos imprescindibles para la finalidad declarada, en coherencia con los criterios de proporcionalidad que exige la EIPD

16.3. Análisis de los riesgos

Analice los apartados 13 y 14 del presente formulario y el resultado del análisis de riesgos, y realice su valoración parcial

El tratamiento de datos personales que se va a llevar a cabo es aceptable desde el punto de vista de los riesgos identificados

SI/NO: Marca **SI** si las medidas aplicadas reducen los riesgos a niveles asumibles; marca **NO** si persisten riesgos altos sin mitigación suficiente.
Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Describa los riesgos identificados y las medidas que los reducen a un nivel aceptable.

Ejemplo de respuesta:

El tratamiento es aceptable desde la perspectiva de riesgos porque, tras identificar amenazas y vulnerabilidades relevantes, se han definido e implantado mitigaciones que reducen el riesgo residual a un nivel asumible, de acuerdo con los requisitos de seguridad del tratamiento del RGPD y la metodología propia de la EIPD

16.4. Análisis de las medidas de seguridad

Analice el apartado 15 del presente formulario y realice su valoración parcial
El tratamiento de datos personales que se va a llevar a cabo es suficientemente seguro considerando las medidas de seguridad aplicadas

SI/NO: Marca **SI** si existen controles adecuados como cifrado, acceso restringido y almacenamiento seguro; marca **NO** si la protección no es suficiente.
Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Indique las medidas que garantizan la confidencialidad, integridad y disponibilidad de los datos.

Ejemplo de respuesta:

El tratamiento es suficientemente seguro porque se han implantado medidas que protegen la confidencialidad, integridad y disponibilidad de la información, coherentes con el artículo 32 del RGPD y con los principios de privacidad desde el diseño y por defecto.

.

16.5. Valoración Final

Considerando las respuestas a las valoraciones parciales anteriores, el impacto que el tratamiento de datos personales que se va a llevar a cabo puede tener en los derechos y libertades de las personas afectadas es razonable y asumible por la universidad

SI/NO: Marca **SI** si el riesgo residual es bajo o razonable y las valoraciones previas son positivas; marca **NO** si persisten riesgos significativos.
Línea explicación: *En caso afirmativo, detalle las razones que lo justifican.* Resuma por qué el impacto es asumible y qué medidas garantizan la protección adecuada de los derechos.

Ejemplo de respuesta:

El impacto que el tratamiento puede tener en los derechos y libertades de las personas afectadas es razonable y asumible por la universidad, considerando las valoraciones parciales previas. Las medidas implantadas —incluyendo seguridad técnica, minimización de datos y transparencia con los interesados— reducen el riesgo residual a un nivel compatible con el RGPD. El tratamiento se realiza con fines legítimos y bajo una base jurídica adecuada. Además, al tratarse de datos sensibles y colectivos potencialmente vulnerables, se aplican medidas reforzadas como el cifrado BitLocker y la conservación separada de la matriz de reidentificación, garantizando una protección robusta y adecuada al riesgo.