RECOGIDA Y PROTECCIÓN DE DATOS PERSONALES DE LOS PARTICIPANTES.

A) Los datos de la investigación no provienen de este proyecto.

☐ Si proceden de un proyecto anterior (especificar):

☐ Otra procedencia (especificar):

Los datos de la investigación se generan en este proyecto y sólo serán utilizados dentro de él.

B) Concrete el procedimiento de captación de las personas participantes:

[Descripción detallada de quién, cómo y cuándo seleccionan a los participantes]

C) Especifique:

☒ Se solicitará **formalmente y por escrito el consentimiento a las personas participantes** del trabajo de campo que formarán parte de la investigación.

☒ Los participantes **disponen de raciocinio para voluntariamente y libremente participar** en el estudio.

☒ Los sujetos participantes **disponen de suficiente información sobre el estudio**.

☒ Explique los **sistemas de información previstos para garantizar este hecho** y si los participantes dispondrán de una hoja informativa en la que quede claramente indicada esta información.

> Se describe al participante, **en lenguaje llano y adaptado a su capacidad de comprensión y cultura general**, en qué consiste el estudio, qué datos se van a obtener, qué riesgos puede tener asociados su realización y cuáles son los resultados que el experimento va a producir.
>
> Se informa al participante de **qué datos de carácter personal se van a obtener y del modo en el que van a estar protegidos**.
>
> Si fuese ese el caso, esta información se daría **también a los representantes legales o tutores del participante**.

☒ Se les informará de que su participación es voluntaria y libre, así como de que pueden retirarse en todo momento, con la consecuente e inmediata eliminación de todos sus registros generados hasta ese momento.

> Se le informará de que en cualquier momento, puede dar por terminada su participación y que todos los **datos relacionados directa o indirectamente con él/ella** son automáticamente destruidos.

☒ Se les informará de los cambios que en el experimento supone su actividad académica y del esfuerzo que conlleva, así como de los posibles inconvenientes y/o beneficios de participar en la investigación.

☒ Se dará a conocer el contacto del comité de Ética a todos los participantes (secretaria.adjunto.vinvestigacion@upm.es).

☒ En el caso de investigación de entornos virtuales, se informará a los participantes de que su comunicación o comportamiento será registrado y será susceptible de análisis.

☒ Se respetará la confidencialidad.

> Todos los datos personales de los participantes así como aquellos relacionados con el momento y lugar en el que se realizan las pruebas, será anonimizado **de modo que no haya modo de relacionar cada uno de los datos obtenidos con el paciente y con el momento/circunstancia en al que se obtuvo**. La información necesaria para reconstruir esa relación estará bajo el control exclusivo del responsable de la protección de Datos Personales en el experimento.
>
> Todos los datos personales en soportes físicos se guardan bajo llave y con acceso exclusivo del responsable de datos, y en soporte digital estarán cifrados con claves bajo el control exclusivo del responsable de Datos

☒ Se respetará el anonimato. La identidad no será relevada si no es bajo consentimiento explícito o bien en el caso de que los datos ya sean públicos, y se informará claramente a los participantes de cómo se

respetará tal anonimato. Explicitar el procedimiento estipulado para salvaguardar el anonimato y la confidencialidad.

A cada participante **se le asignará al azar un código específico único en el momento de su alta** en el experimento.

La lista física/lógica con esos **códigos y cualquier dato personal (nombre apellidos, domicilio, numero de teléfono, cualquier dato biométrico, DNI, certificaciones oficiales, etc.)** estarán bajo el control exclusivo del Responsable de Datos que será el encargado de protegerlo y mantenerlo en secreto.

☒ Una vez finalizado el proyecto está previsto informar de los resultados obtenidos a los participantes del mismo.

Una vez terminado el proyecto todos los datos personales serán destruidos de forma confirmada: **trituración y barajado de soportes físicos** (papel, soportes fotográficos, registros de todo tipo, etc.), y **sobre escritura repetida de toda la capacidad de almacenamiento** y un **formateado a bajo nivel** al final (con por parte de la controladora del dispositivo) de los **sistemas de memoria** (discos duros internos, externos, móviles, memorias USB, teléfonos móviles, etc.) **que hayan albergado en algún momento alguno de esos datos**.

GESTIÓN Y CUSTODIA DE LOS DATOS RECOGIDOS.

¿Está previsto un plan para el tratamiento, la custodia y la conservación de los datos recogidos en el trabajo de campo? En caso afirmativo, realice una breve descripción de ese tratamiento:

Para la gestión de los datos personales se identificará a un responsable de Datos que será parte integrante del equipo de investigación. En su defecto, este papel lo jugará el investigador principal del proyecto que deberá estar formado para la gestión de datos personales y conocer la normativa que se le aplica.

La disponibilidad de todos los datos obtenidos o generados en el proyecto estará protegida por un **procedimiento periódico de salvaguardia (*backup*)** que asegure su recuperación frente a los riesgos más importantes que se enfrentan (robo, destrucción involuntaria, pérdida, etc.). **Tanto los originales como todas su copias se trataran del mismo modos en lo que se refiere a la protección de la confidencialidad e integridad** de los mismos (**los datos siempre estarán cifrados**)

Siempre que sea posible, los datos personales se utilizarán anonimizados y sólo por personal autorizado vinculado al proyecto y que tenga relación con el Laboratorio responsable. Cuando no sea posible el tratamiento con datos anonimizados, el proceso lo tendrá que realizar el responsable de Datos o un equipo autorizado por él/ella y bajo su supervisión directa, de modo que asegure que no haya ningún tipo de fuga o alteración de los datos.

Todos los datos del proyecto deben estar **almacenados en ordenadores** (de sobremesa, portátiles o tablets) **con el medio de almacenamiento** (disco duro, discos de estado sólido, etc.) **cifrados bajo el control de una o varias contraseñas que sólo conocerán los investigadores autorizados** por causa de necesidad para utilizar esos equipos.

Cada uno de los investigadores dispondrá de una **cuenta de usuario distinta, personal e intransferible protegida mediante una contraseña sólo conocida por dicho usuario autorizado**.

La complejidad de las contraseñas no será inferior a **12 caracteres alfanuméricos elegidos al azar** entre las letras mayúsculas, minúsculas, los dígitos y símbolos de puntuación disponibles en el teclado de la máquina.

Esos equipos **sólo estarán encendidos y con sesiones abiertas cuando algún investigador autorizado esté trabajando con ellos**. A menos que sea estrictamente necesario y se cumplan las medidas para ello, estos equipos funcionaran **desconectados de cualquier red local** (cableada, WiFi, Bluetooth, etc.)

¿Qué datos personales se colectan, almacenan y procesan?

Indicar todos los datos personales que se solicitan a los participantes. **Indicar cuál es el procesado al que van a ser sometidos y cuáles son los datos resultantes del procesado de cualquiera de ellos** dentro del desarrollo del proyecto (nombre y apellidos, domicilio actual o anteriores, genero, edad, NIF, estadio físico, nivel de estudios, religión, sexualidad, diestro o zurdo, patologías diagnosticadas, medicación, antecedentes médicos, marcas en la piel y tatuajes, etc.)

¿Se da de alta la existencia de dichos repositorios de datos personales en la Agencia Española de Protección de Datos?

> Todos los ficheros conteniendo datos personales deben darse de alta ante la Agencia Española de Protección de Datos y deben seguir las normas procedimentales y técnicas que dicha agencia tenga marcados.

¿Cuándo se colectan los datos personales?

> Indicar dónde, cuándo, cómo y ante quién se recolectan los datos personales de los participantes.

¿En qué formato se almacenan esos datos personales? (ficheros office, Excel, comprimidos ZIP/RAR, bases de datos, copias en papel, fotografías, registros multimedia, etc.)

> Indicar **explícitamente y de forma completa todos aquellos soportes físicos** (papel, fotografías, registros sonoros analógicos, etc.) **y lógicos** (ordenadores, cámaras digitales, memorias USB o SD, etc.) en los que se va a **almacenar, procesar o transmitir datos personales**. También es necesario indicar bajo qué **formatos y aplicaciones** (fieros Office, Excel, comprimidos ZIP/RAR u otros, bases de datos, etc.) se hace cada una de esas operaciones.

¿Se hacen copias de los ficheros conteniendo datos personales? ¿Cuántas copias se hacen y cómo se gestionan? ¿Cómo se detecta la perdida de alguna copia y como se reacciona ante ese hecho?

> Indicar cuál es la **política de copias** que se va a seguir, cuál la política de **inventario de soportes** que se van a utilizar y cuál el **registro de custodia de dichos soportes/copias**. Aquí es necesario demostrar que no se puede dar el caso de que **se pierda alguna de las copias** y/o que **alguien no autorizado tenga acceso a ellas**, sin **que el responsable de Datos no se dé cuenta de ello**.
>
> Esto debe hacerse tanto con las copias en soporte físico como en digital y, en cualquier caso, **los soportes digitales deben estar siempre convenientemente cifrados** bajo el control de claves criptográficas o contraseñas sólo conocidas per el responsable de datos o personal autorizado por él/ella.

¿En qué lugar o lugares se almacenan los datos personales y cuáles son sus soportes físicos? (PC fijo o portátil, equipo off-line, servidor en red, repositorio en la nube, discos magnéticos removibles, memorias USBs, DVD/CDs, papel, etc.),

> Enumerar soportes, copias, tipos y ubicaciones de todo aquello que almacene o procese datos personales o datos relacionados con ellos, dentro del proyecto.

¿Cómo se recuperan los datos? (acceso directo al ordenador, conexión remota, obtención de copias, etc.)

¿Se pueden recuperar los datos personales a través de una red o a través de Internet?

> Indicar aquí cómo se acceden los datos y muy especialmente a través de que interfaz se hace; por ejemplo, (1) **desde el monitor y teclado conectados al equipo aislado**, (2) mediante **conexión remota dentro de una misma red de área local** en la que está el equipo que contiene/procesa los datos o (3) **a través de una conexión remota a través de Internet**.
>
> Aquí hay que indicar explícitamente **cómo se realizan las copias de seguridad y la restauración de las mismas desde el punto de vista de la conexión**, y por dónde y cómo transitan los datos.

¿Dónde se ubican los servidores o repositorios que guardan los datos personales? (Instalaciones particulares, de la UPM, en España o en la Unión Europea, otros países)

> Es necesario indicar **cuántos, cuáles son y dónde están ubicados los servidores y equipos informáticos** que se van a utilizar en el desarrollo del proyecto. Es también necesario indicar que equipo de comunicaciones (routers, switches, enlaces, redes, etc.) los unen entre sí y con los usuarios que los utilizan.
>
> Es muy importante **dejar claramente establecido por donde viajan y donde residen todos los datos del proyecto** en lo que a ser **dentro o fuera de España y la Unión Europea** se refiere.

¿Cuándo se recuperan datos y para qué fin?

> Indicar en que momento, **para que y quien recupera/extrae datos** de los sistemas como parte del desarrollo del proyecto. Es necesario **establecer cuál es el riesgo de que** (1) alguien **acceda indebidamente** a los mismos y (2) que se **hagan copias no autorizadas** de los datos.

¿Quién o quienes están autorizados a recuperar los datos y cómo demuestran que son los que pretenden ser? (tipos de usuarios, identificación, autenticación, contraseñas, tarjetas de identificación, biometría, registro de actividad en *logs*, etc.)

> Enumerar los responsables con acceso a los datos, su relación con el proyecto.
>
> Indicar cuál es el **mecanismo con el que se autentican frente al sistema** (usuario/contraseña, doble factor de autenticación, tarjeta inteligente, token criptográficos, biometría, etc.) así como la **política de renovación y caducidad de esos derechos e identidades**.

¿Para qué se recuperan los datos personales y cómo se procesan?

> Indicar dentro de los objetivos del proyecto la finalidad de recuperación de los datos, consulta a bases de datos o procesado de los mismos, de modo que quede clara cuáles se utilizan, cómo se utilizan y sobre todo qué producen desde el punto de vista de ser o no datos personales en sí mismos.

¿Los resultados que se obtiene de su procesado, pueden considerarse a su vez datos personales según la ley?

> Hay que tener en cuenta que **el procesado de datos personales anonimizados puede terminar produciendo un dato personal no anónimo**. Aquí hay que descartar razonadamente esta posibilidad.

¿Qué registros indelebles generan las operaciones de almacenamiento y recuperación? (sistema de *log* o bitácoras)

> El sistema operativo utilizado en los equipos de trabajo (sobremesa, portátiles, tabletas, etc.) deberá tener un **sistema de registro de actividades** (Winodws, Linux, MacOS, etc.) que deberá estar **correctamente configurado y activado en todo momento**.
>
> Ese sistema de registro deberá tomar nota de todas las **aperturas y cierres de sesión** que se produzcan, **identificando al usuario**, y **todas las operaciones de creación, borrado, modificación y copia de los ficheros** contenidos en la **partición donde se guardan todos los ficheros relacionados con el proyecto**, **incluidos los temporales que puedan generar** las aplicaciones de procesado de los mismos. Quedan fuera de este registro las operaciones con ficheros directamente relacionados con el funcionamiento del propio sistema operativo.
>
> **Nadie excepto el responsable de los Datos podrá acceder a los registros de ese sistema** y será su responsabilidad **analizarlos periódicamente para confirmar que todos los accesos que se han realizado son reconocidos como correctos** y que no hay anomalía alguna en el funcionamiento del sistema.

¿Qué medidas anti-modificación tienen esos registros de actividad? ¿Qué impide que alguien pueda cambiarlos o impedir que se generen?

> Indicar cuál es la configuración que se da al sistema de registro de actividades (*logging*) y mostrar que con ello es **suficiente para controlar quien accede a los datos, cuando lo hace, desde donde lo hace y lo que a fin de cuentas hace con ellos**.

¿Dónde y cómo se almacenan los registros de acceso a los datos personales?

> Muchas veces, para mayor seguridad, **los registros de actividad se mandan o se replican en otros equipos para asegurar la disponibilidad de los mismos**. Indicar en este punto si existe esa duplicación de los registro s y cómo se ha organizado.
>
> Resaltar las cualidades que tiene el sistema en cuanto a **impedir que los registros se pierdan, en general o selectivamente, o que se modifiquen** de algún modo.

Indicar con detalle cómo se hacen anónimos los datos personales recolectados o los derivados de ellos.

> **Describir con todo detalle cómo los datos personales se convierten en un conjunto de datos anónimos**. Justificar por qué el conocimiento de todos o algunos de los datos del proyecto no permiten reconocer la persona a los que pertenecen. Es necesario justificar que realmente se anonimizan los datos **y que permanecen así durante toda la existencia del proyecto**.

¿Cómo se transportan los datos personales en su comunicación a los usuarios o servicios que los procesen?

> Indicar **si se hace y cómo se transfieren los datos de una ubicación a otra**, **de un equipo a otro**; a través de conexiones de red (directas o indirectas), de sistemas de almacenamiento que van de un sitio a otro (**discos portátiles, memorias USB, etc.**), de almacenamientos interpuestos como es el caso de los **servicios en la nube**, si se hace por correo electrónico, o por cualquier otro procedimiento de mensajería.

¿Cómo se identifican a los destinatarios de dichas transferencias?

> Toda transferencia de datos tiene un destinatario y un remitente, en este punto hay que indicar **mediante qué mecanismos se comprueba que el remitente y el destinatario son los que tiene que ser**. En es necesario clásicos, basta con que se conozcan en persona los que intercambian el medio de transporte, pero en canales telemáticos hay que tomar especial cuidado en identificar con quien se está hablando y de quien se reciben cosas. **En cualquier caso, los datos transferidos siempre deberán estar cifrado en reposo (almacenados) y su integridad ser verificable**.

¿Qué medidas concretas se toman para evitar fugas de información?

> Indicar y enumerar las **medidas específicas que se toman para evitar que los datos del proyecto puedan terminar fuera de las instalaciones del proyecto y/o en manos de personal no autorizado**.
>
> Los mecanismos más utilizados son (1) el **aislamiento físico y lógico** de los equipos y redes en los que se desarrolla el proyecto, (2) la **verificación de autenticidad e inventario de soportes** para la transferencia y almacenamiento de los datos, (3) la **monitorización continua** de los datos y (4) **el permanente cifrado de los datos** tanto en almacenamiento como en transporte,

¿Si se utilizan repositorios de información conectados a Internet es necesario saber cómo se protege la confidencialidad de su contenido, su integridad y cómo se controla quién y cuándo accede a los mismos? (Dropbox, Google Drive, Amazon S3, Azure, iCloud, Box, etc.)

> En el caso de utilizar **Internet o los servicios que hay en ella**, tanto si son específicos como es el caso de correo electrónico, como si son generales, como **la recolección de datos (formularios web), computación (procesado de datos) y almacenamiento o transferencia a través de la Nube**, es preciso **describirlo con todo detalle** ya que este tipo de prácticas tiene asociados grandes riesgos.
>
> En cualquier caso, es mejor **evitar el uso de este tipo de tecnologías cuando se trabaja con datos personales**.

¿Qué operaciones de salvaguardia (*backup*) se realizan y cómo se protege la integridad y confidencialidad de esas copias de seguridad?

> Describir el proceso de generación de copias de seguridad, la frecuencia y extensión con las que se realizan y cuáles son las pruebas y procesos de restauración que se realizan/ensayan. Recordar que todas las copias de seguridad deben estar correctamente cifradas y firmadas, bajo el control exclusivo del responsable de Datos.

¿Cómo se destruyen las copias con datos personales cuando dejan de ser necesarias o se termina el proyecto? ¿Cómo se asegura la destrucción de todas las copias?

> Indicar cómo se **destruyen todos los soportes físicos** en los que se hayan almacenado o transferido datos personales, así como los **procedimientos de borrado seguro** que se aplican en todos los medios de almacenamiento digital. Describir el **proceso de revisión de inventario** y la correspondiente **destrucción física de los medios digitales** una vez terminado el proyecto.