ANEXO XX. CONTRATO O ACTO JURÍDICO DE ENCARGO DEL TRATAMIENTO DE DATOS PERSONALES

En _____, a [__] de _____ de 202_.

REUNIDOS

De una parte, D./D.ª _____, en calidad de _____, actuando en nombre y representación de la Universidad _____,, y domicilio a efectos de notificaciones en _____,, en nombre y representación de la misma, actuando de conformidad con las competencias que le atribuyen los Estatutos de la Universidad (en adelante, *Universidad* o *Responsable del Tratamiento*).

De otra Parte, D./D.ª _____, en calidad de _____, actuando en nombre y representación de [RAZÓN SOCIAL], con NIF _____, sociedad constituida de acuerdo con la legislación española, con domicilio social en calle [DOMICILIO SOCIAL], (en adelante, *Encargado del Tratamiento*).

Ambas Partes se reconocen mutuamente la capacidad legal bastante para suscribir este contrato/ CONVENIO y quedar obligadas en la representación en que respectivamente actúan, y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del Tratamiento es una entidad especializada en _____.

II.- Que, en el marco de dicha actividad, las Partes han suscrito un [Convenio | Contrato de Servicios cuya oferta (Oferta/Nº expediente _____) ha sido aceptada con fecha _____], y en virtud del cual el Encargado se compromete a prestar el/los siguiente/s servicio/s;

[Descripción del servicio contratado].

EL ENCARGADO DEL TRATAMIENTO designa como persona de contacto a los efectos del presente contrato a ……..

Por su parte, [EL RESPONSABLE] designa como persona de contacto a los efectos del presente contrato a ……..

III.- Que para la prestación de los servicios descritos en el Expositivo anterior, es inherente que el Encargado tratamiento trate datos de carácter personal por cuenta del Responsable.

IV.- Que de conformidad con el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD), y del artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD); a través del presente se definen las obligaciones y responsabilidades que asume el Encargado en el tratamiento de los datos de carácter personal, con arreglo a las siguientes:

ESTIPULACIONES

PRIMERA. - OBJETO Y FINALIDAD DEL ENCARGO DE TRATAMIENTO.

Mediante el presente acuerdo/contrato/convenio se habilita al ENCARGADO del tratamiento, para tratar por cuenta del RESPONSABLE, los datos de carácter personal necesarios para prestar el servicio indicado en el Expositivo II del presente Contrato.

[Incluir:
Denominación del Tratamiento:
Nombre y email del Responsable Delegado del Tratamiento y/o persona del Servicio donde se realice el tratamiento de datos].

SEGUNDA.-. TIPOS DE DATOS PERSONALES Y CATEGORIAS DE INTERESADOS AFECTADOS

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE del tratamiento autoriza al ENCARGADO del tratamiento a tratar en su nombre y según lo dispuesto a continuación la información referenciada, necesaria para prestar el servicio acordado:

CATEGORÍAS DE DATOS PERSONALES

(Marcar con una X la categoría de datos que vaya a tratar la otra parte. Eliminar los datos en amarillo que no apliquen)

☐ Datos identificativos:

Nombre y Apellidos, DNI o NIE, Dirección, Teléfono, Dirección de Correo Electrónico, IP, imagen...

☐ Características personales:

Fecha y lugar de nacimiento, edad, estado civil, sexo, datos familiares, nacionalidad, idioma…

☐ Circunstancias sociales:

Aficiones, hábitos, forma de vida, propiedades, inscripciones…

☐ Información académica o profesional:

Formación, titulaciones, expediente académico…

☐ Detalles del empleo:

CV, vida laboral, puesto de trabajo, experiencias laborales anteriores …

☐ Información comercial:

Informes con datos personales, estadísticas que identifiquen al individuo…

☐ Información económico-financiera y de seguros:

Datos bancarios, ingresos, rentas, ayudas, becas, prestaciones, créditos, préstamos, avales, plan de pensiones, jubilación…

☐ **Categorías especiales de datos:**

Origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, datos relativos a la vida sexual o la orientación sexual de una persona física…

☐ **Datos personales relativos a condenas e infracciones penales:**

Expediente o historial judicial, sanciones, procedimientos judiciales…

CATEGORIAS DE INTERESADOS

(Marcar con X los colectivos de los que la otra parte va a tratar datos. En caso de 'otros' especificar el colectivo al que se hace referencia).

☐ Estudiantes

☐PAS

☐Participantes en proyectos de investigación

☐PDI

☐Antiguos estudiantes

☐Otros: _____

☐ Ciudadanos nacionales

☐ Extranjeros comunitarios

☐ Extranjeros no comunitarios.

☐ Sujetos vulnerables: Menores de edad.

☐ Otros sujetos vulnerables (ancianos, menores, personas con discapacidad, víctimas de violencia de género, personas participantes en programas de inserción laboral o reinserción social, refugiados políticos, titulares de derecho de asilo u otro tipo de protección similar, etc)

☐ Empleados por cuenta propia o ajena.

☐ Profesionales de sectores específicos (educación, salud…) Empleado públicos. Altos cargos de la administración. Directivos de empresas. Representantes electos. Cargos políticos

☐ Consumidores de bienes y servicios de uso corriente.

☐ Pacientes sometidos a tratamientos sanitarios. Usuarios de servicios sociales.

☐ Personas condenadas penalmente.

☐ Personas definidas en función de sus hábitos (deportistas, coleccionistas, aficionados a determinados eventos, usuarios de redes de contacto social…)

☐Otros: _____

OPERACIONES DE TRATAMIENTO DE DATOS

☐ Recogida

☐ Registro

☐ Organización

☐ Estructuración

☐ Conservación

☐ Adaptación o modificación

☐ Extracción

☐ Consulta

☐ Utilización

☐ Difusión o cualquier otra forma de habilitación de acceso

☐Cotejo o interconexión

☐ Limitación

☐ Supresión o destrucción

☐ Comunicación por transmisión

☐ Otros (especificar)

TERCERA. - DURACIÓN.

El presente acuerdo entrará en vigor a la fecha de su firma y permanecerá vigente mientras persista la prestación de servicios que origina la firma del presente encargo de tratamiento.

CUARTA. - OBLIGACIONES DEL ENCARGADO.

El ENCARGADO y todo el personal bajo su control se obliga a:

1. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

2. Tratar los datos de acuerdo con las instrucciones documentadas del RESPONSABLE. Si el Encargado del tratamiento considera que alguna de las instrucciones infringe cualquier disposición en materia de protección de datos debe informar inmediatamente al Responsable.

3. [OPCIÓN 1:] No realizar transferencias internacionales de datos objeto del presente acuerdo.

[OPCIÓN 2:] Si el ENCARGADO, En el caso de que los servidores o servicios que precisan de la transferencia de datos personales a un tercer país por parte del Encargado están ubicados fuera del Espacio Económico Europeo (EEE), éste informará por escrito al RESPONSABLE de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

Además, el ENCARGADO solicitará un informe a su delegado o delegada de Protección de Datos. El informe del DPD seguirá los criterios descritos en las Recomendaciones 01/2020 del Comité Europeo de Protección de Datos y tendrá en cuenta aspectos como el nombramiento de un representante en los términos descritos en el art. 24.1 CE. 27 del RGPD en caso de que el encargado no resida en la UE. El informe del DPD deberá ser tenido en cuenta por el responsable del tratamiento antes de autorizar el tratamiento fuera de la EEE. El tratamiento fuera del EEE por parte del Encargado sólo se podrá llevar a cabo si se dispone de una autorización expresa y firmada del Responsable del tratamiento.

RAZÓN SOCIAL	**DATOS CONTACTO**	**TERCER PAIS**	**GARANTIA (ver Art. 46 a 49 RGPD)**

4. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del RESPONSABLE, que contenga, conforme al artículo 30.2 del Reglamento (UE) 2016/670:

- El nombre y los datos de contacto del ENCARGADO y de cada Responsable por cuenta del cual actúe el ENCARGADO.
- Las categorías de tratamientos efectuados por cuenta de cada Responsable.
- Una descripción general de las medidas técnicas y organizativas de seguridad apropiadas que esté aplicando al tratamiento de los datos.

5. No comunicar los datos a terceras personas, ni siquiera para su conservación, salvo en los supuestos legalmente admisibles.

El Encargado puede comunicar los datos a otros encargados del tratamiento del propio Responsable, de acuerdo con sus instrucciones. En este caso, el Responsable debe identificar, previamente y por escrito, a la entidad a la que se deben comunicar, qué datos comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el Encargado se viera en la necesidad de comunicar datos personales a un tercero, debe solicitar autorización expresa al Responsable del Tratamiento. Si en un plazo de 10 días naturales no ha obtenido respuesta, se dará por denegado tal permiso.

6. [OPCIÓN 1:] No subcontratar total ni parcialmente el servicio contratado. En caso de que sea necesario que el Encargado del Tratamiento subcontrate parte del mismo para su mejor desarrollo, y eso conlleve un tratamiento de datos personales objeto del presente encargo por la parte subcontratada, es necesario que el Encargado solicite autorización previa y expresa y por escrito al Responsable del Tratamiento indicando los tratamientos que se pretenden subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto; en cuyo caso se deberá anexar al presente el correspondiente contrato o acuerdo de subencargo de tratamiento. Si en un plazo de 10 días naturales no ha obtenido respuesta, se dará por denegado tal permiso.
[OPCIÓN 2:] Siendo necesario para la correcta prestación del servicio, el Encargado del Tratamiento (Encargado inicial) queda autorizado a recurrir al /los siguiente/s subencargado/s del tratamiento:

RAZÓN SOCIAL	**DATOS DE CONTACTO**	**TRATAMIENTO**

El subcontratista, también ostenta la condición de Encargado del tratamiento, por lo que necesariamente debe cumplir las obligaciones establecidas en el presente contrato,
Es el Encargado inicial quién debe regular esta nueva relación de manera que la entidad subencargada quede sujeta a las mismas condiciones y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el Encargado inicial seguirá siendo plenamente Responsable ante el Responsable del tratamiento.

7. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.

8. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, entre las que se encuentra recibir formación necesaria en materia de protección de datos personales; o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria. El Encargado mantendrá a disposición del Responsable la documentación acreditativa del cumplimiento de estas obligaciones.

9. Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad de datos ante el ENCARGADO, éste debe comunicarlo al Responsable mediante [*Según procedimiento establecido en cada universidad*]

- La obligación de contestar estos derechos corresponde al Responsable del tratamiento.
- La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.
- El ejercicio de derechos ante el Encargado requerirá la previa presentación por parte del interesado de documento identificativo. En caso de no presentarlo, se le requerirá por escrito antes de notificar al Responsable. Para el derecho de acceso el Encargado facilitará al Responsable la lista de los datos personales de que se disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del Responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.
- Una vez recibido un ejercicio de derechos, el Encargado paralizará su tratamiento hasta que el Responsable estudie y conteste al interesado/afectado, y le informe sobre cómo debe proceder con los datos personales objeto del ejercicio de derecho.

El Encargado informará a todo el personal que trate datos por cuenta del Responsable acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos y teniendo en cuenta la manera de proceder.

10. Cuando el Encargado tenga conocimiento de que ha sufrido un incidente de seguridad que ha afectado a datos personales del Responsable del tratamiento, el Encargado notificará al Responsable, sin dilación indebida y a no mas tardar en 24 horas desde que se tenga conocimiento del incidente y a través de [*dirección facilitada por el Responsable*], facilitando como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- Datos de la persona de contacto del ENCARGADO para obtener más información.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

El ENCARGADO asistirá al Responsable con toda la información de la que disponga, a la hora de realizar la comunicación de las violaciones de la seguridad tanto ante la Autoridad de Control como a los interesados, si procede.

11. Colaborar y poner a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones por parte del Responsable u otro auditor autorizado por él.

12. Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. Las medidas de seguridad mínimas a aplicar por el ENCARGADO se recogen en la estipulación SEXTA de este acuerdo.

13. En caso de que el tratamiento a realizar incluya la recogida de datos personales el Encargado del tratamiento debe facilitar, en el momento de recoger estos datos, la información relativa a los tratamientos de datos que se llevarán a cabo. La redacción y el formato en el que se facilitará la información debe consensuarse con el Responsable del tratamiento, antes de iniciarse la recogida de datos personales.

14. Colaborar con el Responsable del tratamiento en la realización de las Evaluaciones de Impacto de la Protección de datos, cuando así proceda.

15. Colaborar con el Responsable del tratamiento en el momento de realizar consultas previas a la Autoridad de Protección de Datos competente, cuando así proceda.

16. En el caso de haber designado un Delegado de protección de datos de acuerdo con el artículo 34 de la LOPDGDD, comunicar su identidad y datos de contacto mediante [_____].
17. Efectuar todas estas obligaciones de manera gratuita, sin coste adicional respecto al de la prestación del servicio.

QUINTA. - OBLIGACIONES DEL RESPONSABLE.

Corresponde al RESPONSABLE:

1. Proporcionar al ENCARGADO los datos necesarios para que pueda prestar el servicio.

2. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del Reglamento (UE) 2016/670, la Ley Orgánica 15/2018 y del resto de normativa aplicable en materia de protección de datos de las personas físicas por parte del ENCARGADO.
3. Supervisar el tratamiento de datos realizado por el ENCARGADO, incluida la realización de inspecciones y auditorías.

SEXTA. - MEDIDAS DE SEGURIDAD MÍNIMAS A APLICAR POR EL ENCARGADO.

[OPCIÓN 1. Implantar las siguientes medidas de seguridad técnicas y organizativas apropiadas para garantizar un nivel de seguridad apropiado al riesgo y de acuerdo con el nivel [ALTO | MEDIO |BAJO] del Esquema Nacional de Seguridad (ENS).

Garantizar las siguientes medidas de seguridad específicas:

- [_____]

En el caso de que se solicite garantizar un cumplimiento de medidas de seguridad acorde con el nivel BAJO del ENS:

- Realizar y mantener documentación acreditativa de haber realizado una autoevaluación inicial y autoevaluaciones posteriores que verifiquen el cumplimiento de los requerimientos previstos en el ENS, al menos cada dos años, o
- Realizar y mantener documentación acreditativa de haber realizado una auditoría con una empresa certificada que verifique el cumplimiento de los requerimientos previstos en la ENS, al menos cada dos años con un nivel como mínimo igual al indicado.

En el caso de que se solicite garantizar un cumplimiento de medidas de seguridad acorde con el nivel MEDIO o ALTO del ENS: realizar y mantener documentación acreditativa de haber realizado una auditoría con una empresa certificada que verifique el cumplimiento de los requerimientos previstos en la ENS, al menos cada dos años con un nivel como mínimo igual al indicado.

Aplicar y mantener documentación acreditativa de estar aplicando las medidas de seguridad específicas requeridas.

Dado que es necesario mantener la acreditación del cumplimiento de las medidas de seguridad durante toda la vida del contrato y sus posibles prórrogas, la Universidad podrá en cualquier momento de la prestación del mismo solicitar la entrega de documentación acreditativa del cumplimiento de las medidas de seguridad. En caso de que este hecho se produzca el Encargado estará obligada a facilitar la información requerida en el plazo de dos semanas. En el caso de existir dudas razonables sobre la veracidad de la documentación aportada, la Universidad podrá realizar por sí misma o encargar a entidades especializadas inspecciones o auditorías de las medidas de seguridad aplicadas por el contratista. Los gastos asociados a estas inspecciones o auditorías irán a cargo del Encargado.

[OPCIÓN 2. Implantación de una norma ISO de seguridad de la información (ISO 27001)

En el caso de que se solicite garantizar un cumplimiento de medidas de seguridad acorde con la implantación de una Norma ISO 27001 de seguridad de la información

En el caso de que se solicite garantizar un cumplimiento de medidas de seguridad: realizar y mantener documentación acreditativa de haber realizado una auditoría con una empresa certificada que verifique el cumplimiento de los requerimientos previstos en la Norma ISO, al menos cada dos años.

Aplicar y mantener documentación acreditativa de estar aplicando las medidas de seguridad específicas requeridas.

Dado que es necesario mantener la acreditación del cumplimiento de las medidas de seguridad durante toda la vida del contrato y sus posibles prórrogas, la Universidad podrá en cualquier momento de la prestación del mismo solicitar la entrega de documentación acreditativa del cumplimiento de las medidas de seguridad. En caso de que este hecho se produzca el Encargado estará obligada a facilitar la información requerida en el plazo de dos semanas. En el caso de existir dudas razonables sobre la veracidad de la documentación aportada, la Universidad podrá realizar por sí misma o encargar a entidades especializadas inspecciones o auditorías de las medidas de seguridad aplicadas por el contratista. Los gastos asociados a estas inspecciones o auditorías irán a cargo del Encargado.

[OPCIÓN 3. Adhesión a códigos de Conducta

Los Encargados podrán adherirse a códigos de conducta, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales.

Dichos Encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

[OPCIÓN 4. El Responsable del tratamiento detalla de manera individualizada las medidas de seguridad que deberá aplicar el Encargado. Modificar el listado según corresponda]

Los ámbitos de aplicación de las medidas mínimas de seguridad que deberá adoptar el ENCARGADO, en las actividades de tratamiento objeto del presente acuerdo, serán:

- Los recursos bajo el control del ENCARGADO (como sistemas informáticos y de archivo, centros de trabajo y trabajadores) y que éste destine al tratamiento de los datos objeto del presente encargo.
- Los recursos bajo el control del Responsable cuando éste haya encomendado al ENCARGADO la seguridad de los mismos.
- Los sistemas de información que el ENCARGADO desarrolle o implante por cuenta del Responsable.

Estas medidas mínimas se enumeran a continuación:

1. **Medidas organizativas**. Tanto la entidad en su condición de Encargado, como todo el personal al que el ENCARGADO proporcione acceso a los datos personales, deberá cumplir y ser informado de las siguientes medidas organizativas:

- Deber de confidencialidad y secreto. Éste persiste incluso cuando finalice la relación laboral o de prestación de servicios.
- Evitar el acceso de personas no autorizadas a los datos personales. A tal fin quedará prohibido: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos

personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia si lo hubiera. Cuando la persona se ausente del puesto de trabajo, procederá al bloqueo de la pantalla o al cierre de la sesión.

- Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día, y serán custodiados cuando, con motivo de su tramitación, se encuentren fuera de los dispositivos o salas de archivo.
- No se desecharán documentos (papel) o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción, de forma que la información no sea recuperable.
- No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
- Se informará sobre la manera de proceder ante ejercicios de Derechos. Este modo de actuar es de obligado cumplimiento.
- Se informará sobre la manera de proceder ante violaciones de seguridad de datos de carácter personal. Cuando se produzcan violaciones de seguridad de datos de carácter personal, como, por ejemplo, el robo o acceso indebido a los datos personales se notificará al Responsable de forma inmediata acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. Asimismo, se apoyará al Responsable a realizar la notificación de la violación de la seguridad a la Agencia Española de Protección de Datos teniendo en cuenta la información a disposición del ENCARGADO.

2. **Medidas de seguridad técnicas, relativas a la identificación**. El ENCARGADO implantará como mínimo las siguientes medidas técnicas para garantizar la identificación y autenticación de los usuarios con acceso a los datos:

- No se permitirá el uso para fines particulares de aquellos ordenadores y dispositivos destinados al tratamiento de los datos personales.
- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador o dispositivo.
- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de contraseñas (o mecanismos equivalentes) para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras, y se renovarán periódicamente (al menos de forma anual).
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

3. **Medidas de seguridad técnicas para salvaguardar los datos**. A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- Actualización de ordenadores y dispositivos. Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados.
- Malware. En los ordenadores y dispositivos donde se realice el tratamiento de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- Cortafuegos. Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un cortafuegos activado en aquellos sistemas en los que se realice el almacenamiento y/o tratamiento de datos personales.
- Cifrado de datos. Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se utilizará previamente un método de cifrado para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- Copia de seguridad. Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el equipo con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

4. **Verificación, evaluación y valoración periódica de las medidas de seguridad**. El ENCARGADO implantará un procedimiento periódico que le permita verificar, evaluar y valorar, la eficacia de las medidas técnicas y organizativas implantadas en los sistemas de tratamiento, centros de trabajo y usuarios bajo su control.

5. De ese procedimiento periódico se derivarán la implantación de **mecanismos adicionales** para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Seudonimizar y cifrar los datos personales, en su caso.
- Las medidas de seguridad abarcarán la protección de los sistemas de información, así como de los sistemas de tratamiento manual y archivo de la documentación.
- La revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual.

El ENCARGADO dispondrá en todo momento de información actualizada sobre las medidas de seguridad aplicadas en el encargo de tratamiento y deberá proporcionarlas al Responsable

cuando éste las solicite y en todo caso siempre que haya cambios relevantes en su arquitectura de seguridad de la información.

En el caso de existir dudas razonables sobre la veracidad de la documentación aportada, la Universidad podrá realizar por sí misma o encargar a entidades especializadas inspecciones o auditorías de las medidas de seguridad aplicadas por el contratista. Los gastos asociados a estas inspecciones o auditorías irán a cargo del Encargado.

SÉPTIMA. - DEVOLUCIÓN DE LOS DATOS.

Una vez finalice el presente acuerdo y según le sea indicado por el Responsable, el Encargado deberá suprimir los datos personales tratados, devolverlos al Responsable o trasmitirlos a otro Encargado designado por éste. El Encargado deberá suprimir cualquier copia que esté en su poder. No obstante, el Encargado podrá mantener una copia con los datos bloqueados mientras puedan derivarse responsabilidades de la ejecución de este acuerdo o el principal que constituye su razón de ser.

OCTAVA. - INCUMPLIMIENTO.

En el caso de que el Encargado de Tratamiento destine los datos a finalidad distinta de las señaladas, los comunique o utilice incumpliendo las estipulaciones del presente contrato, será considerado a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente ante las autoridades competentes y los interesados.

El incumplimiento por parte del Encargado de las obligaciones referidas en el presente acuerdo comportará que responda directamente ante las Autoridades de Protección de Datos, o ante cualquier tercera persona de las infracciones que se puedan haber cometido derivadas de la ejecución del presente acuerdo y/o del cumplimiento de la legislación vigente en materia de protección de datos de carácter personal.

NOVENA. - LEGISLACIÓN Y JURISDICCIÓN.

El presente acuerdo se regirá e interpretará conforme a la legislación española en todo aquello que no esté expresamente regulado, sometiéndose las partes, para las controversias que pudieran surgir en relación al mismo, a la competencia de los Juzgados y Tribunales de [_____], con renuncia a cualquier otro fuero que les pudiera corresponder.

Y en prueba de conformidad, las partes suscriben el presente contrato, en duplicado ejemplar y a un solo efecto, en la ciudad y fecha al inicio indicados.

Por la UNIVERSIDAD	**Por [RAZÓN SOCIAL ET]**
D./Dª. _____	**D./Dª. _____**