MANUAL DE PROTECCIÓN DE DATOS

FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO LA PAZ

Conforme a las obligaciones establecidas en:

• 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
• Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD)

Fecha adaptación: 11 de septiembre de 2018

Fecha de actualización: 26 de diciembre de 2023

ÍNDICE

1. Instrucciones a seguir por el cliente tras la entrega de la documentación de adaptación a la normativa de protección de datos

FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO LA PAZ (en adelante "FIBHULP") debe comprometerse a cumplir con lo dispuesto en el presente Manual de Protección de Datos y realizar un seguimiento periódico de dicho cumplimiento.

Independientemente de lo dispuesto en este Manual de Protección de Datos, FIBHULP queda obligada y es responsable de cumplir con la normativa estatal y europea vigente de protección de datos.

Es especialmente importante subrayar que FIBHULP es plenamente responsable de decidir e implantar correctamente las medidas organizativas y técnicas necesarias para cumplir y poder demostrar que se cumple con lo dispuesto en la normativa estatal y europea vigente de protección de datos, especialmente en el Reglamento General de Protección de Datos (**RGPD**) y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD).

Por ello, se recomienda encarecidamente llevar a cabo las siguientes acciones:

- Mantener actualizado el Registro de Actividades de Tratamiento recogido en el **Anexo I**.
- Mantener actualizada la Relación de Usuarios del **Anexo II**. En caso de que los usuarios de los sistemas sean modificados en un futuro, deberán añadirse o eliminarse de dicho Anexo.
- Mantener actualizada la lista de prestadores de servicios del **Anexo III.**
- Completar el Registro de Incidencias del **Anexo IV** en caso de existir alguna incidencia que pueda afectar a la seguridad de los datos personales (robo de datos, eliminación accidental de datos, accesos no autorizado, etc.).
- Mantener actualizado el Inventario de soportes del **Anexo V** (activos de información con datos personales, documentación en papel, archivos, ordenadores, discos duros, etc.).
- Completar el Registro de entrada y salida de soportes del **Anexo VI**, siempre que se produzca una entrada o salida de soportes con datos personales desde o hacia fuera de las instalaciones de la Fundación.
- Completar el Registro de Accesos del **Anexo VII**, principalmente cuando se realicen tratamientos de datos sensibles.
- Revisar periódicamente el cumplimiento de lo dispuesto en el presente Manual de Protección de Datos y completar el Registro del **Anexo VIII**.
- Completar el Registro de Delegación de Autorizaciones del **Anexo IX**.
- El personal con acceso a datos personales debe firmar el Recibo del Manual de Protección de Datos del **Anexo X**.
- Permitir que los interesados puedan ejercer eficazmente sus derechos de protección de datos y atender a la mayor brevedad posible las solicitudes de ejercicio de dichos derechos. Para ello, se puede hacer uso de los modelos recogidos en los **Anexos XI, XII y XIII**.

- Nombrar al Delegado de Protección de Datos (DPO), en su caso, Responsables Funcionales, Responsable de Seguridad Técnico y Gestor de Solicitudes de Ejercicio de Derechos. Para ello, se puede hacer uso de las plantillas recogidas en el **Anexo XIV**.
- Utilizar las cláusulas de protección de datos recogidas en el **Anexo XV** para informar y, en caso de ser necesario, solicitar el consentimiento de los interesados (empleados, candidatos, clientes, investigadores, proveedores, etc.). Se recomienda que, si es posible, cada uno de estos interesados firme la cláusula correspondiente, de forma que la Fundación guarde evidencia de haber cumplido con el derecho de información exigido en el RGPD y en la LOPD-GDD.
- Seleccionar con diligencia debida a los Encargados del Tratamiento que presten servicios con acceso a datos personales, de forma que quede garantizado que tales Encargados del Tratamiento cumplen con la normativa vigente de protección de datos. Además, la Fundación puede utilizar los contratos recogidos en el **Anexo XVI** con Proveedores que presten servicios con o sin acceso a datos personales y con Clientes a los que la Fundación preste servicios con acceso a datos personales.
- Notificar a la Agencia Española de Protección de Datos (AEPD) y, en su caso, a los interesados, las violaciones de seguridad que afecten a los derechos y libertades de los individuos. Para ello, se puede hacer uso de la plantilla recogida en el **Anexo XXVII**.
- Completar periódicamente el Formulario de Verificación del **Anexo XXVIII** para cada Actividad de Tratamiento, con el objetivo de evaluar la necesidad de realizar una Evaluación de Impacto relativa a la protección de datos personales (EIPD).
- Eliminar los datos cuando hayan pasado los plazos de conservación establecidos por una Ley o por FIBHULP. En el **Anexo XIX** se recoge un recopilatorio de plazos indicativos de conservación de los datos.

Tenga en cuenta que la adaptación se hace en un momento concreto. Si FIBHULP sufre cambios, nuevas líneas de negocio, o recoge una nueva tipología de datos, contacte con una empresa consultora experta en protección de datos ya que es probable que deban darse nuevos pasos sobre la adaptación de su Fundación a la normativa.

2. Introducción al Manual de Protección de Datos

En el presente Manual de Protección de Datos se recogen la política, procedimientos y medidas necesarias para cumplir con las exigencias 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 (**Reglamento General de Protección de Datos o RGPD**) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD), aplicable a los tratamientos de datos personales realizados por FIBHULP en su condición de Responsable del Tratamiento o de Encargado del Tratamiento.

Para la determinación de esta política, procedimientos y medidas, han sido tenidas en cuenta las pautas fijadas en el RGPD y en la LOPD-GDD, en atención a la naturaleza, alcance, contexto y fines de los datos personales tratados y las medidas expresadas en la recogida de información que ha realizado la empresa ALARO AVANT, S.L. en FIBHULP. La Fundación dispone de 15 días naturales para expresar las disconformidades que pudiese detectar en la redacción del presente documento a la empresa consultora, pasados los cuales se entenderá como correcto el contenido. Cualquier modificación posterior del contenido del presente documento será realizado por la empresa consultora en la revisión anual.

Las medidas recogidas en el presente Manual de Protección de Datos serán adoptadas e implantadas por FIBHULP, tal y como le compete en su condición de Responsable o de Encargado del Tratamiento, salvo las que expresamente hayan sido delegadas en el presente documento a un Encargado del Tratamiento o Subencargado del Tratamiento si así se cita.

Es necesario mantener este Manual de Protección de Datos actualizado en todo momento, lo que supone realizar revisiones de forma periódica para contemplar posibles cambios relevantes que se pudieran producir, así como verificar el cumplimiento de lo dispuesto en el presente documento.

3. Definiciones

A los efectos del presente Manual de Protección de Datos se establecen las siguientes definiciones reflejadas por el RGPD:

- **autoridad de control**: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51 (Autoridad de Control);
- **autoridad de control interesada**: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:
  a. el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
  b. los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o
  c. se ha presentado una reclamación ante esa autoridad de control;
- **consentimiento del interesado**: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;
- **datos biométricos**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;
- **datos genéticos**: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;
- **datos personales**: toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;
- **datos relativos a la salud**: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;
- **destinatario**: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será

conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

- **elaboración de perfiles**: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;
- **empresa**: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;
- **encargado del tratamiento o encargado**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;
- **establecimiento principal**:
  a. en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;
  b. en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al RGPD;
- **fichero**: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
- **grupo empresarial**: grupo constituido por una empresa que ejerce el control y sus empresas controladas;
- **limitación del tratamiento**: el marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro;
- **normas corporativas vinculantes**: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

- **objeción pertinente y motivada**: la objeción sobre la existencia o no de infracción del RGPD, o sobre la conformidad con el RGPD de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;
- **organización internacional**: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo;
- **representante**: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27 (Representantes de responsables o encargados del tratamiento no establecidos en la Unión), represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del RGPD;
- **responsable del tratamiento o responsable**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;
- **servicio de la sociedad de la información**: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo ;
- **seudonimización**: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;
- **tercero**: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;
- **tratamiento transfronterizo**:
  a. el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o
  b. el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión,

pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

- **tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;
- **violación de la seguridad de los datos personales**: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

4. Política de Protección de Datos

4.1. Objeto

La presente Política tiene por objeto fundamental establecer las reglas relativas al tratamiento de datos personales por parte de **FIBHULP** en el ejercicio legítimo de sus actividades empresariales.

Los Procedimientos recogidos en el **Apartado 6** del presente Manual de Protección de Datos desarrollarán esta Política de Protección de Datos, estableciendo y regulando las medidas y procedimientos que **FIBHULP** debe implantar para el correcto cumplimiento del RGPD, de la LOPD-GDD y otras disposiciones estatales y europeas en protección de datos personales.

4.2. Ámbito de aplicación

En el presente apartado del Manual de Protección de Datos se describe, conforme establece el artículo 2 del RGPD y el artículo 2 de la LOPD-GDD, el ámbito en el que resultan de aplicación las medidas aquí recogidas.

La delimitación del ámbito de aplicación se hace conforme a tres criterios básicos:

- **Ámbito Material**

Este Manual de Protección de Datos es de aplicación única y exclusivamente a FIBHULP con domicilio social en Paseo de la Castellana 261, 28046 de Madrid.

El presente Manual de Protección de Datos será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser tratados por **FIBHULP**.

La política, procedimientos y medidas recogidas en el presente Manual de Protección de Datos podrán ser extendidas a cualesquiera otras instalaciones que **FIBHULP** pudiera crear y en las que se llevasen a cabo cualquier tipo de tratamiento de datos personales así como en aquellas otras personas jurídicas que presten servicios al responsable del tratamiento o sean encargados del tratamiento de este, tal y como establece el Capítulo IV del RGPD y el Título V de la LOPD-GDD.

En el tratamiento de los datos personales, es preciso garantizar la seguridad, mediante el control de los accesos a los datos, a través de cualquier vía que lo permita.

La normativa contenida en el presente Manual se aplica a todos los recursos de los sistemas de información por medio de los cuales se puede acceder a datos personales, así como todo dispositivo que efectúe cualquier proceso de tratamiento o almacenamiento de datos personales.

Se entiende por "recurso" cualquier parte componente del sistema de información. Dichos recursos son los siguientes:

- ❑ Servidores.
- ❑ Ordenadores de sobremesa (PC's de usuarios) y dispositivos móviles (portátiles, tablets, smartphones).
- ❑ Intranet.
- ❑ Conexión a red externa (internet).
- ❑ Sistemas operativos y aplicaciones instaladas para acceder a los datos.
- ❑ Impresoras.
- ❑ Soportes para copia o almacenamiento de datos, incluidas las arquitecturas que las soportan.
- ❑ Todo tipo de soportes magnéticos propiedad de la Fundación, programas informáticos, archivos que contengan datos personales y programas que traten los mismos.
- ❑ Documentación de la Fundación que se encuentre registrada en soporte manual, como documentación en papel, etc.

- **Ámbito Personal**

Se encuentran obligadas al cumplimiento de las prescripciones legales conforme a las cuales se redacta el presente Manual de Protección de Datos, las siguientes personas:

- Quienes presten servicios, ya sea de forma directa o indirecta, en **FIBHULP**, cualquiera que sea la naturaleza de la relación jurídica que le una con la misma.
- Toda persona que, por la labor que desempeñe, tenga o pueda tener acceso a las instalaciones o departamentos donde están ubicados los sistemas de información a través de los cuales se tratan datos personales.

La Fundación se hace responsable de la labor de formar e informar a las personas que, por su condición de usuarios, se encuentren bajo el ámbito de aplicación del presente Manual de Protección de Datos, sobre el adecuado cumplimiento de lo establecido en el mismo.

El Responsable del Tratamiento, ha establecido una relación de usuarios (**Anexo II**) en la que se hacen constar los datos de los usuarios, los cuales debido a sus funciones desarrolladas en la Fundación, tienen acceso y tratan los datos personales.

Dicha relación será actualizada a fin de que responda con veracidad a la situación existente en cada momento en la Fundación, con respecto a la identificación de los usuarios.

- **Ámbito Territorial**

El presente Manual de Protección de Datos se aplica al tratamiento de datos personales en el contexto de las actividades de **FIBHULP**, como Responsable o Encargado del Tratamiento, independientemente de que el tratamiento tenga lugar en la Unión Europea o no.

4.3. Principios relativos al tratamiento de datos personales

Los principios relativos al tratamiento de datos personales, conforme al artículo 5 RGPD, son:

- **Principio de licitud, lealtad y transparencia:** este principio está vinculado al derecho de información, ya que ésta debe facilitarse a los interesados de forma comprensible y accesible. **FIBHULP**, como Responsable del Tratamiento, solamente podrá efectuar, lícitamente, tratamiento de datos personales, si se cumple, al menos, una de las siguientes condiciones:
  - Ha obtenido el consentimiento del interesado para uno o varios fines específicos. Corresponderá a **FIBHULP** demostrar que el interesado prestó su consentimiento para cada una de las finalidades, por cualquier medio de prueba admisible en derecho.
  - El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación, a petición de éste, de medidas precontractuales.
  - El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al Responsable del Tratamiento.
  - El tratamiento es necesario para proteger intereses vitales del interesado.
  - El tratamiento es necesario para el cumplimiento de una misión realizada en interés público, al que está obligado el Responsable del Tratamiento.
  - El tratamiento es necesario para la satisfacción de intereses legítimos del Responsable del Tratamiento, o para un tercero al que se comunican los datos personales, siempre que sobre tales intereses no prevalezcan los intereses o derechos y libertades

fundamentales del interesado. Para realizar esta ponderación de intereses deben tenerse en cuenta las expectativas razonables de los interesados basadas en su relación con el Responsable del Tratamiento. Los interesados conservarán sus derechos, y en particular, el derecho a ejercer la oposición al tratamiento, si consideran que prevalecen sus derechos y libertades frente a dicho interés legítimo del Responsable del Tratamiento.

- **Principio de limitación de la finalidad:** los datos deberán ser recogidos con fines determinados, explícitos y legítimos de **FIBHULP**, como Responsable del Tratamiento, y no serán tratados, posteriormente, de manera incompatibles con dichos fines.
- **Principio de minimización de los datos:** los datos deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Principio de exactitud:** los datos deberán ser exactos y puestos al día por parte de **FIBHULP**, como Responsable del Tratamiento. Se presumirán exactos y actualizados los datos obtenidos directamente del interesado.
- **Principio de limitación del plazo de conservación:** los datos deberán ser mantenidos por **FIBHULP**, como Responsable del Tratamiento, de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del Tratamiento.
- **Principio de integridad y confidencialidad:** los datos serán tratados de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito, o contra su pérdida, destrucción o daño accidental. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los posibles riesgos para los derechos y libertades de las personas físicas, **FIBHULP**, como Responsable o Encargado del Tratamiento, establecerá las medidas técnicas y organizativas apropiadas para garantizar un nivel adecuado del riesgo. Para lograr este nivel adecuado, **FIBHULP** debe valorar la implantación de las siguientes medidas:
  - la seudonimización y el cifrado de datos personales
  - la capacidad de garantizar la confidencialidad, la integridad y la disponibilidad de los datos, y la resiliencia de los sistemas y servicios de tratamiento
  - la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico
  - las medidas de seguridad adicionales que, en su caso, resulten aplicables, del presente Manual de Protección de Datos
  - las medidas de seguridad adicionales que, en su caso, vengan exigidas por la legislación local aplicable al Responsable o al Encargado del Tratamiento
  - el proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento

- la adhesión a un Código de Conducta o a un mecanismo de Certificación, conforme a la normativa de protección de datos, podrá servir como medio de prueba del cumplimiento de los requisitos de seguridad exigibles

- **FIBHULP** y todas las personas que intervengan en cualquier fase del tratamiento de datos personales están sujetos al deber de confidencialidad de los datos que, en su caso, será un deber complementario a los deberes de secreto profesional que les incumban. Este deber de confidencialidad tendrá carácter indefinido, aun cuando hubiese finalizado la relación del obligado con **FIBHULP**.
- **Principio de responsabilidad proactiva: FIBHULP**, como Responsable o Encargado del Tratamiento, deberá mantener una responsabilidad proactiva en relación al cumplimiento de todos los principios relativos al tratamiento de datos personales, incluidos en la normativa estatal y europea de protección de datos, así como en el presente Manual de Protección de Datos; es decir, **FIBHULP** está directamente obligado a dicho cumplimiento y debe ser capaz en todo momento de demostrar dicho cumplimiento.
- **Principio de privacidad por defecto y desde el diseño: FIBHULP** debe aplicar los principios de tratamiento de datos por defecto y desde el diseño, con anterioridad al inicio del tratamiento y también mientras se esté desarrollando. Desde el mismo momento en que se diseña un producto o servicio que implique el tratamiento de datos personales, hay que evaluar el impacto de dicho tratamiento en la protección de los datos de los interesados, y se deben tomar las medidas organizativas y técnicas necesarias para integrar en el tratamiento las garantías que permitan aplicar de forma efectiva los principios establecidos en el RGPD, en la LOPD-GDD, en las leyes estatales y europeas y en el presente Manual de Protección de Datos.

4.4. Funciones y Obligaciones

4.4.1. Funciones y obligaciones del Responsable del Tratamiento

FIBHULP, ostenta la condición de Responsable del Tratamiento, por cuanto detenta íntegramente la facultad de decisión sobre la finalidad, contenido y uso en el tratamiento de datos personales.

Se detallan a continuación las obligaciones atribuidas legalmente a **FIBHULP** por su condición de Responsable del Tratamiento:

- Realizar por sí mismo, o a través de un representante o del Delegado de Protección de Datos, en su caso, o por medio de persona autorizada al efecto, cualesquiera de las gestiones de notificación ante la Agencia Española de Protección de Datos (AEPD).
- Redactar y establecer en la Fundación la aplicación y el cumplimiento del presente Manual de Protección de Datos, así como completar la documentación de protección de datos de aquellas otras personas jurídicas sobre las que realice tratamiento de datos, como encargado del tratamiento, siempre que los realice en sus propios locales.
- Velar por el cumplimiento de todos los principios, derechos y obligaciones establecidos en el RGPD y en la LOPD-GDD; en particular permitir a los interesados (titulares de los datos personales), el ejercicio de sus derechos en protección de datos (acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición).
- Nombrar a un Delegado de Protección de Datos, en su caso, que, entre otras funciones, supervise el cumplimiento del RGPD y de la LOPD-GDD.
- Nombrar a los Responsables Funcionales correspondientes para cada Actividad de Tratamiento.
- Nombrar al Responsable de Seguridad Técnico.
- Nombrar al Gestor de Solicitudes de Ejercicio de Derechos.

La designación del Delegado de Protección de Datos, en su caso, y del resto de Responsables no supone la exoneración de responsabilidad para el Responsable del Tratamiento por incumplimiento de la normativa reguladora en materia de protección de datos personales.

4.4.2. Funciones y obligaciones del Delegado de Protección de Datos

FIBHULP ha acordado la designación del siguiente **Delegado de Protección de Datos (DPO)**:

Alaro Avant, S.L.

La Fundación, en su condición legal de Responsable del Tratamiento y/o Encargado del Tratamiento, está obligada a designar un Delegado de Protección de Datos (DPO) en los siguientes supuestos:

- Tratamiento llevado a cabo por una autoridad u organismo públicos
- Tratamiento a gran escala de datos sensibles, como actividad principal
- Condenas e infracciones penales, como actividad principal
- Observación habitual y sistemática de interesados a gran escala, como actividad principal

El DPO no estará sujeto a ninguna instrucción por parte del Responsable o Encargado del Tratamiento, y estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, en materia de protección de datos.

Las funciones principales del DPO son:

- Informar y asesorar al Responsable o Encargado del Tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD, de la LOPD-GDD y de otras disposiciones de protección de datos estatales y europeas.
- Supervisar el cumplimiento del RGPD y de la LOPD-GDD, así como de otras disposiciones de protección de datos estatales y europeas, y del presente Manual de Protección de Datos Personales, incluida la asignación de responsabilidades, la concienciación y la formación del personal que participe en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de Datos (EIPD) y supervisar su aplicación.
- Cooperar con la Agencia Española de Protección de Datos (AEPD).
- Actuar como punto de contacto con la AEPD para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Comunicar a la Agencia Española de Protección de Datos (AEPD) y, en su caso, a los interesados, las violaciones de seguridad que puedan entrañar daños y perjuicios físicos, materiales o inmateriales a personas físicas.

Otras funciones del DPO son:

- Controlar a los Responsables Funcionales, al Responsable de Seguridad Técnico y al Gestor de Solicitudes de Ejercicio de Derechos, y supervisar que cumplen con sus funciones en protección de datos personales.
- Informar a los Responsables Funcionales y al Responsable de Seguridad Técnico sobre cualquier asunto que considere relevante, para la gestión de la protección de datos, especialmente si supone un riesgo para los derechos y libertades de los Interesados.
- Consultar y colaborar en la implantación de las medidas acordadas en el presente Manual de Protección de Datos y, en general, en el RGPD y en la LOPD-GDD.
- Redactar las cláusulas informativas correspondientes para permitir hacer efectivos los derechos de los individuos.
- Redactar los contratos de prestación de servicios con acceso a datos y asesorar para que la selección de los encargados del tratamiento se realice con diligencia debida, de forma

que quede garantizado que se cumple con la normativa estatal y europea vigente de protección de datos, especialmente con lo dispuesto en el RGPD y en la LOPD-GDD.

- Formar y concienciar al personal en materia de protección de datos personales.
- Delegar cuando considere necesario las funciones que el **Anexo IX** del presente Manual de Protección de Datos le atribuye como DPO.

4.4.3. Funciones y obligaciones de los Responsables Funcionales

FIBHULP nombrará un Responsable Funcional para cada Actividad de Tratamiento descrita en el **Anexo I** del presente Manual de Protección de Datos.

Actividad de Tratamiento	Responsable Funcional
Gestión de I+D+I	Sara Fernández
Difusión de I+D+I	Sara Fernández
Alumnos	Sara Fernández
Ponentes	Sara Fernández
Sugerencias y Reclamaciones	Sara Fernández
RRHH	María Quintanar y Ana Herrera
PRL	María Quintanar y Ana Herrera
Canal de denuncias	María Quintanar y Paloma Gómez Campelo
Proveedores	Mónica García López y Laura López
Selección de personal	María Quintanar y Ana Herrera
Clientes	Mónica García López y Laura López
Investigadores	Sara Fernández
Reembolso y compensación de gastos	Mónica García López y Laura López
Donaciones	Sara Fernández
Biobanco	Paloma Gómez Campelo
Pacientes en proyectos de investigación	Marisa Tejedor
Órganos de Gobierno	Sara Fernández

Las funciones principales de los Responsables Funcionales son:

- Ejecutar lo dispuesto en la normativa estatal y europea vigente en protección de datos y, especialmente, en el RGPD y en la LOPD-GDD, así como en el presente Manual de Protección de Datos.
- En lo que le afecte y siguiendo el procedimiento establecido en el apartado 6.3. del presente Manual de Protección de Datos, controlar, verificar y realizar un seguimiento del cumplimiento de dichas normas, así como de las medidas organizativas que **FIBHULP**, como Responsable o Encargado del Tratamiento, haya decidido implantar.

- Completar, mantener actualizado y garantizar la veracidad del Registro de Actividad de Tratamiento del **Anexo I** del que haya sido nombrado Responsable Funcional, según **Anexo XIV** del presente Manual de Protección de Datos.
- Comunicar al Responsable del Tratamiento o al DPO, en su caso, cualquier modificación realizada en el Registro de Actividad de Tratamiento que le corresponde, así como cualquier nueva actividad que implique la creación de un nuevo Registro de Actividad de Tratamiento.
- Consultar con el Responsable del Tratamiento o con el DPO, en su caso, el modelo de cláusulas informativas y/o de solicitud del consentimiento a utilizar.
- Informar a los interesados, a través de las correspondientes cláusulas informativas, del tratamiento de sus datos personales por parte de **FIBHULP**.
- Consultar con el Responsable del Tratamiento o con el DPO, en su caso, las cláusulas a utilizar en los contratos de prestación de servicios con Encargados del Tratamiento.
- Solicitar la autorización del Responsable del Tratamiento o del DPO, en su caso, para comunicar datos personales a terceros no autorizados.
- Atender las solicitudes de ejercicio de derechos de los interesados y remitírselas a la persona responsable de gestionar dichas solicitudes, de forma que **FIBHULP** garantice a los interesados el ejercicio efectivo de sus derechos.
- Colaborar con el Responsable del Tratamiento y con el DPO, en su caso, en la formación y concienciación del personal de **FIBHULP** en protección de datos personales.
- Informar a todas las personas con acceso a datos personales de su Actividad de Tratamiento sobre el procedimiento a seguir para atender las solicitudes de ejercicio de derechos de protección de datos, tal y como se recoge en el **Apartado 7** del presente Manual de Protección de Datos.
- Comunicar inmediatamente al Responsable del Tratamiento o al DPO, en su caso, las violaciones de seguridad que puedan entrañar daños y perjuicios físicos, materiales o inmateriales a personas físicas, enviándole completado el modelo de notificación que se acompaña como **Anexo XVII** al presente Manual de Protección de Datos.
- Comprobar la correcta aplicación de los procedimientos recogidos en el **Apartado 6.2.** del presente Manual de Protección de Datos:
    - Procedimiento de control de acceso físico a datos personales y a los locales donde se encuentren ubicados los soportes no automatizados. Entre otras funciones, debe supervisar la correcta custodia de soportes no automatizados y de documentos en papel en mobiliario apropiado.
    - Procedimiento de notificación, registro y gestión de incidencias. Entre otras funciones, debe registrar y comunicar al Responsable del Tratamiento o al DPO, en su caso, las incidencias que puedan afectar a los derechos y libertades de los individuos y, en su caso, al Responsable de Seguridad Técnico cualquier incidencia técnica que pueda afectar a datos personales.

- Procedimiento de gestión de soportes. Entre otras funciones, debe autorizar la entrada y salida de soportes, con datos personales de su Actividad de Tratamiento, fuera de los locales en los que están ubicados.
- Procedimiento de copias o reproducción de documentos con datos sensibles. Entre otras funciones, debe autorizar las recuperaciones de datos personales de su Actividad de Tratamiento.
- Procedimiento de seudonimización.

- Delegar cuando considere necesario las funciones que el **Anexo IX** del presente manual de Protección de Datos le atribuye como Responsable Funcional.

4.4.4. Funciones y obligaciones del Responsable de Seguridad Técnico

FIBHULP ha acordado la designación del siguiente **Responsable de Seguridad Técnico**, encargado de supervisar la correcta implantación de las medidas de seguridad en los sistemas de información de la Fundación:

Servicio de Informática del Hospital Universitario La Paz

Las funciones principales del Responsable de Seguridad Técnico son:

- Ejecutar lo dispuesto en la normativa estatal y europea vigente en protección de datos y, especialmente, en el RGPD y en la LOPD-GDD, así como en el presente Manual de Protección de Datos.
- En lo que le afecte y siguiendo el procedimiento establecido en el apartado 6.3. del presente Manual de Protección de Datos, controlar, verificar y realizar un seguimiento del cumplimiento de dichas normas, así como de las medidas técnicas que **FIBHULP**, como Responsable o Encargado del Tratamiento, haya decidido implantar.
- Comprobar la correcta aplicación de los procedimientos recogidos en el **Apartado 6.1.** del presente Manual de Protección de Datos:
  - Procedimiento de configuración de ordenadores y dispositivos.
  - Procedimiento de control de acceso. Entre otras funciones, debe:
    - aplicar las medidas adecuadas de control de acceso físico a los locales donde se encuentren ubicados los sistemas de información con datos personales, así como autorizar la presencia de terceros en dichos locales,
    - asegurar la efectiva aplicación del procedimiento de identificación y autenticación de usuarios,

- conceder, alterar o anular el acceso autorizado a datos personales y a recursos que puedan contener datos personales, de acuerdo con los criterios establecidos por el Responsable del Tratamiento,
- elaborar y mantener actualizada una relación de usuarios que tienen acceso autorizado al sistema informático de la compañía, con especificación del nivel de acceso que tiene cada usuario. En la actualidad esta relación de usuarios es llevada a cabo a través del **Anexo II** del presente Manual y/o a través del Directorio Activo o del gestor de usuarios de las respectivas aplicaciones,
- asegurar la efectiva asignación, distribución y almacenamiento de contraseñas vigentes, en forma ininteligible, y el mantenimiento de la confidencialidad de las mismas, así como su modificación periódica,
- asegurar que el sistema limita el acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones; así como comprobar la correcta aplicación de los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.

- Procedimiento de gestión de soportes. Entre otras funciones, debe:
  - mantener actualizado el Registro de entrada y salida de soportes informáticos,
  - identificar, inventariar y almacenar en lugar seguro los soportes informáticos que contienen datos personales,
  - comprobar la aplicación de las medidas de seguridad que se deban adoptar cuando un soporte informático vaya a ser desechado o reutilizado, de tal modo que se impida la recuperación posterior de la información almacenada en los mismos,
  - comprobar que se imposibilita la recuperación indebida de la información almacenada en soportes informáticos que vayan a salir fuera de los locales en que se encuentre ubicado el sistema de información.
- Procedimiento de gestión de incidencias. Entre otras funciones, debe:
  - registrar las incidencias que le sean notificadas y mantener actualizado dicho Registro,
  - gestionar y asegurar la resolución efectiva de la incidencia a la mayor brevedad posible,
  - comunicar al Responsable del Tratamiento o al DPO, en su caso, las incidencias que puedan afectar a los derechos y libertades de los individuos.
- Procedimiento de copias de seguridad. Entre otras funciones, debe:
  - asegurar la efectiva realización de copias de respaldo y recuperación de datos, y el cumplimiento de la periodicidad establecida para ello.
  - hacer un seguimiento del registro de incidencias y ampliar los campos del mismo para dejar constancia de los procedimientos realizados para la recuperación de los

datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos han sido necesarios grabar manualmente en el proceso de recuperación.

- Procedimiento de realización de pruebas con datos. Entre otras funciones, debe:
  - asegurar que en la fase de pruebas de los sistemas de información, éstas no se efectúen con datos personales reales salvo que pueda asegurarse el mismo nivel efectivo en la aplicación de medidas de seguridad.
- Procedimientos de seudonimización y cifrado.
- Procedimiento para establecer un plan de contingencias.

- Comunicar inmediatamente al Responsable del Tratamiento o al DPO, en su caso, las violaciones de seguridad que puedan entrañar daños y perjuicios físicos, materiales o inmateriales a personas físicas, enviándole completado el modelo de notificación que se acompaña como **Anexo XVII** al presente Manual de Protección de Datos.
- Delegar cuando considere necesario las funciones que el **Anexo IX** del presente manual de Protección de Datos le atribuye como Responsable de Seguridad Técnico.

4.4.5. Funciones y obligaciones del Personal o Usuarios

Se considera ***usuario*** *al sujeto autorizado para acceder a datos personales o recursos que contienen datos personales.*

Aquella persona que, por prestar sus servicios para **FIBHULP**, tenga autorizado el acceso a los sistemas de información con datos personales facilitados por los interesados, quedará sujeto al control de su actividad por parte del Delegado de Protección de Datos (DPO) o del Responsable Funcional correspondiente.

Todo el personal o usuario con acceso a los datos personales está obligado a cumplir las prescripciones establecidas en el presente Manual de Protección de Datos y en la normativa estatal y europea vigente de protección de datos personales.

Las funciones y obligaciones del personal son:

- **Cumplimiento del presente Manual de Protección de Datos**
  - Todo el personal con acceso a datos personales debe colaborar en la correcta implantación de las medidas, organizativas y técnicas, necesarias para cumplir con lo dispuesto en el presente Manual de Protección de Datos y en la normativa estatal y europea vigente de protección de datos personales.
  - En caso de plantearse dudas sobre la implantación de dichas medidas, debe consultarse al Responsable Funcional correspondiente o, en su caso, al Delegado de Protección de Datos.

- Todos y cada uno de los empleados de **FIBHULP** habrán de firmar un recibo (**Anexo X**) del presente Manual de Protección de Datos, una vez les haya sido facilitado y hayan tenido ocasión de leerlo, informándose así de todas las obligaciones a las que quedan sujetos como consecuencia del tratamiento de datos personales que realizan en el cumplimiento de sus funciones.

- Llevar a cabo, cuando así se haya delegado, las funciones que el **Anexo IX** del presente Manual de Protección de Datos le atribuye como Usuario Autorizado.

- **Deber de confidencialidad y secreto**

  - Debe evitar el acceso de personas no autorizadas a datos personales:

    - evitar dejar los datos personales expuestos a terceros, como pantallas electrónicas desatendidas, documentos en papel o soportes en zonas de acceso público, pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia, etc.

    - proceder al bloqueo de la pantalla o al cierre de la sesión cuando se ausente del puesto de trabajo.

  - Queda absolutamente prohibida la utilización, divulgación o cesión de los datos de los interesados para finalidades diferentes a aquellas para las que hubieren sido facilitados.

  - Queda absolutamente prohibido revelar, permitir o facilitar el acceso a datos personales o cualquier otra información personal a terceras personas ajenas a **FIBHULP** sin autorización del titular de dichos datos, así como a otros trabajadores de la Sociedad que, por sus funciones, no tengan autorizado el acceso a los datos personales. Debe prestarse especial atención a no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.

  - En caso de plantearse dudas sobre el acceso a datos personales por parte de terceras personas, debe consultarse al Responsable Funcional correspondiente o, en su caso, al Delegado de Protección de Datos.

  - Este deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la Sociedad.

  - Todas la información y soportes que contenga datos personales relacionadas con las actividades de la Sociedad son propiedad de la misma, estando obligado todo trabajador a devolverlos cuando así le sea solicitado por **FIBHULP** y, en cualquier caso, con motivo de la extinción del contrato de trabajo.

- **Solicitudes de ejercicio de derechos**

  - Atender las solicitudes de ejercicio de derechos de los interesados y remitírselas al Responsable Funcional correspondiente o a la persona responsable de gestionar dichas solicitudes, de forma que **FIBHULP** garantice a los interesados el ejercicio efectivo sus derechos.

- **Recogida de datos personales**
  - Queda absolutamente prohibido recopilar información acerca de otras personas, incluidas las direcciones de correo electrónico, sin su consentimiento o sin que exista una habilitación legal que permita el tratamiento de los datos.
  - Siempre que se recojan datos personales deben utilizarse las cláusulas informativas recogidas en los **Anexos XV** del presente Manual de Protección de Datos.
  - En caso de plantearse dudas sobre la recogida de datos personales y las cláusulas a utilizar, debe consultarse al Responsable Funcional correspondiente o, en su caso, al Delegado de Protección de Datos.
- **Copias de seguridad**
  - Para la correcta realización de las copias de seguridad según el procedimiento descrito en este Manual de Protección de Datos, todo el personal de **FIBHULP** debe trabajar guardando la información que contenga datos personales en los servidores de **FIBHULP**.
  - Está prohibido guardar cualquier otro tipo de información, ya sea personal o que no sea relativa a su trabajo, en los servidores de **FIBHULP**, así como almacenar datos de negocio o datos personales en los equipos personales, ya que su sustracción pondría en riesgo a la empresa, considerándose al usuario el único responsable, en caso de incurrir en este caso.
- **Incidencias**
  - Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad e integridad de los datos personales, sistemas, soportes informáticos y archivos (estén automatizados o no).
  - Es obligación de todo el personal que preste sus servicios para **FIBHULP**, comunicar al Responsable Funcional correspondiente o al Responsable de Seguridad Técnico cualquier incidencia que se produzca en los sistemas de información, independientemente de la relevancia que tenga. Dicha comunicación deberá realizarse a la mayor brevedad posible desde el momento en el que se produce la incidencia o se tenga certeza de que pudiera producirse.
- **Violaciones de seguridad de datos personales**
  - Comunicar inmediatamente al Responsable Funcional correspondiente o al Responsable de Seguridad Técnico, incluso si es necesario al Delegado de Protección de Datos (DPO) las violaciones de seguridad que puedan entrañar daños y perjuicios físicos, materiales o inmateriales a personas físicas, enviándole completado el modelo de notificación que se acompaña como **Anexo XVII** al presente Manual de Protección de Datos.
- **Uso de documentos en papel y soportes**
  - Los documentos en papel y los soportes que contengan datos personales deben almacenarse en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.

- Cada documento en papel y cada soportes deberá custodiarse en el lugar que le corresponde, de forma que no sean visibles y accesibles a terceros no autorizados.

- Todo los trabajadores serán responsables de la debida custodia de la llave, tarjeta o mecanismo de apertura del mobiliario o local donde se encuentran ubicados los documentos en papel o los soportes.

- No deben desecharse documentos o soportes con datos personales sin garantizar su destrucción.

- **Uso de las claves de acceso**

  - Las claves o contraseñas de los usuarios con acceso a datos personales son siempre individuales, personales e intransferibles, por lo que queda absolutamente prohibido comunicarlas a cualquier otra persona, salvo autorización expresa del Responsable Funcional correspondiente o, en su caso, del Delegado de Protección de Datos (DPO).

  - Si el usuario tiene conocimiento de que otra persona conoce alguna de sus claves de acceso a datos personales, deberá ponerlo inmediatamente en conocimiento del Responsable Funcional correspondiente o del Responsable de Seguridad Técnico, con el fin de que le sea asignada una nueva clave de acceso y se proceda a cancelar la anterior. En caso de incumplimiento de esta obligación, el usuario será el único responsable de los actos realizados por la persona que utilice de forma no autorizada su identificador.

  - Queda absolutamente prohibido intentar acceder a datos personales, aplicaciones, archivos o unidades de red que el usuario tenga restringidas de los sistemas informáticos de la Sociedad o de terceros.

- **Uso del correo electrónico**

  - El correo electrónico tan sólo podrá ser utilizado, para llevar a cabo las tareas que sean encomendadas directamente a cada persona, sin que, en ningún caso, pueda ser utilizado para fines particulares, salvo autorización del Responsable Funcional correspondiente.

  - Se declara expresamente la inseguridad del correo electrónico a través de Internet, al poder ser los mensajes objeto de falsificaciones y suplantaciones de personalidad. Todo usuario, siempre que haga uso del correo electrónico, debe cumplir al menos con las siguientes medidas:

    - El usuario deberá utilizar, siempre y cuando sea posible, métodos de cifrado y mecanismos fiables de autenticación en la transmisión de información con datos personales a través de correo electrónico, principalmente si se trata de datos sensibles.

    - Nunca se deberán abrir archivos adjuntos que provengan de un origen desconocido, ya que podrían contener virus o código que desestabilicen el sistema.

    - Siempre se ha de cerrar la sesión de cada programa de correo una vez se haya terminado de utilizar el mismo. De esta forma, se puede impedir que intrusos no deseados tengan acceso a la cuenta de cada usuario.

- No se ha de responder a mensajes no solicitados u otro tipo de correo ofensivo o de acoso. Respondiendo se confirma que la dirección de correo electrónico está activa y se le puede enviar constantemente correo electrónico no solicitado.

- Queda absolutamente prohibido enviar mensajes de correo electrónico de forma masiva (spam) o con fines comerciales o publicitarios, sin el conocimiento de los interesados y del Responsable Funcional correspondiente.

- Interceptar correo electrónico de otros usuarios para intentar leerlo, borrarlo, copiarlo o modificarlo. Esta actividad puede constituir delito de interceptación de las telecomunicaciones, tipificado en el artículo 197 del Código Penal.

- Enviar o reenviar mensajes en cadena en la red corporativa de **FIBHULP** o redes externas, sin la debida autorización del Responsable Funcional correspondiente.

- **Uso de Internet**

  - El sistema informático, la Intranet y los terminales utilizados por los usuarios son titularidad de **FIBHULP**. Esta exclusiva titularidad permite a la Sociedad comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada en la misma por cualquier usuario, cumpliendo en tales situaciones, las exigencias legales que legitiman dicha actividad.

  - El acceso a páginas web, grupos de noticias, listas de distribución y otras fuentes de información queda restringido a las materias estricta y directamente relacionadas con las funciones que desempeña cada trabajador dentro de la Sociedad.

  - Con el objeto de evitar intromisiones indebidas, deben utilizarse los programas de navegación más actualizados y activar aquellas opciones que informen de la existencia de mecanismos ajenos que tienen como objetivo la obtención ilícita y no consentida de datos. No obstante, para evitar incompatibilidades en el sistema será necesario consultar con el Responsable de Seguridad Técnico de forma previa a la actualización o instalación de cualquier tipo de Software o aplicación no autorizada.

  - Queda absolutamente prohibido introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos, sin autorización expresa por parte del Responsable Funcional correspondiente y sin solicitar el asesoramiento del Responsable de Seguridad Técnico.

  - Utilizar los recursos telemáticos de **FIBHULP** (incluida las redes Internet e Intranet) para actividades que no se hallen directamente relacionadas con el puesto de trabajo asignado a cada usuario.

  - Recomendaciones para la seguridad de los usuarios en Internet:

    - Utilizar un gestor de contraseñas
    - Crear contraseñas seguras
    - Utilizar la autenticación en dos pasos
    - Evitar enviar las contraseñas por mail. Utilizar un método más seguro
    - Encriptar tus dispositivos móviles (portátil, Smartphone, Tablet…)
    - Usar una VPN

- Revisar la privacidad en tu entorno: usar una pantalla de privacidad en el dispositivo móvil, cubrir la cámara web, etc.
- Utilizar navegadores que respetan la privacidad a través de ventanas privadas: Safari, Brave, Firefox, Tor
- Utilizar buscadores que bloquean los rastreadores publicitarios y mantienen el historial de forma privada: DuckDuckGo
- Usar un proveedor de correo electrónico que respete tu privacidad: FastMail, ProtonMail, Tutanota
- Revisar los permisos de privacidad de tus dispositivos (ubicación, cámara, micrófono, fotos, salud…)
- Revisar la privacidad/seguridad de tus navegadores, cuentas de correo electrónico, redes sociales…
- Revisa y elimina los metadatos adjuntos a las fotos que compartes
- Utilizar mensajería cifrada punto a punto: Signal, iMessage
- Tener precaución cuando recibas posibles mensajes de phising

- **Uso de aplicaciones**

  - Únicamente podrán utilizarse aquellas aplicaciones creadas por el personal de **FIBHULP** para uso propio o aquellas aplicación de las que se haya obtenido la correspondiente licencia de uso por quien legalmente es titular de los derechos de explotación.

  - Queda terminantemente prohibido utilizar dichas aplicaciones para uso particular de los trabajadores.

- **Uso de dispositivos móviles**

  - Aquellos usuarios que dispongan de smartphones o cualquier dispositivo móvil (tablets, etc.) con capacidad para leer el correo electrónico, utilizar contactos, o acceder a datos de la empresa deberán extremar las precauciones para evitar su robo o pérdida. Es importante hacer un uso correcto y configurar en el terminal las máximas medidas de seguridad posibles, para que en caso de sustracción o pérdida, evitar que se pueda acceder a datos sensibles de la empresa o acceder a cualquier información relevante (contactos, correos, historial de llamadas, calendario, documentos, etc.):

    - Como norma general, ante cualquier sospecha de robo o pérdida, se deberá comunicar de forma inmediata al Responsable de Seguridad Técnico para que realicen los trámites necesarios para, en caso de que sea posible, hacer un borrado remoto o impedir el acceso al terminal. Además, se deberá presentar la correspondiente denuncia y comunicarlo al Responsable de Seguridad Técnico para su conocimiento al tratarse de una posible incidencia de protección de datos.

    - Queda prohibido configurar el correo electrónico o utilizar contactos/calendarios profesionales en dispositivos personales, que no sean propiedad de la empresa.

    - Si por algún motivo el terminal es compartido o usado por otra persona, no se podrá configurar el correo electrónico, ni utilizar el calendario o contactos (profesionales). Se deberán eliminar todos los datos y hacer un borrado del terminal antes de entregarlo a otra persona (incluyendo las tarjetas de datos o de memoria adicionales que puedan llevar).

- Queda prohibido almacenar en las tarjetas de memoria ficheros o datos de la empresa.

- Queda prohibido revelar información personal a través de redes sociales cuando se accede desde dispositivos de la empresa. Su uso estará restringido a temas profesionales.

- Es obligatorio configurar en el terminal donde esté configurado el correo electrónico (mails o contactos/calendario) o cualquier otro software desde el que se pueda acceder a documentación de la empresa (Dropbox, onedrive, etc.) un bloqueo complejo mediante pin, contraseña, o cualquier otro programa que impida el uso del terminal por cualquier persona que no sea el propietario.

- **Otras medidas de seguridad**

  - Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de **FIBHULP** o de las bases de datos de terceros. Dichos actos pueden constituir un delito de daños, tipificado en el artículo 264.2 del Código Penal.

  - Introducir voluntariamente programas, virus, caballos troyanos, gusanos, bombas de relojería, robots de cancelación de noticias, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen, o sean susceptibles de causar, cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tendrá la obligación de utilizar los programas antivirus establecidos en la Sociedad e implantados por el Responsable de Seguridad Técnico y estar al tanto de sus actualizaciones periódicas, para prevenir la entrada en el sistema informático de cualquier virus destinado a borrar o alterar los datos alojados en los sistemas informáticos implantados en la Sociedad.

  - Instalar copias ilegales de cualquier programa sin la correspondiente licencia preceptiva o sin la autorización del titular de los derechos de autor del mismo.

  - Desinstalar, eliminar o inutilizar cualquier programa que esté instalado legalmente en los sistemas informáticos de la Empresa, sin la correspondiente autorización del Responsable de Seguridad.

- **Incumplimiento de las obligaciones**

El incumplimiento de las obligaciones anteriormente descritas dará lugar a la imposición de las correspondientes sanciones disciplinarias por parte de Sociedad.

FIBHULP podrá hacer efectivas las medidas establecidas en el Artículo 20 del Estatuto de los Trabajadores sobre control de la actividad laboral, por lo que la Sociedad podrá adoptar las

medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.

Por ello, la Sociedad podrá utilizar cualquier evidencia que obre en su poder (correo electrónico, acceso a internet, instalación de aplicaciones, grabación de imágenes, etc.) en sede disciplinaria laboral.

Las sanciones serán las previstas por el Convenio Colectivo vigente en cada momento aplicable al Responsable del Tratamiento y por el texto refundido del Estatuto de los Trabajadores en lo referente a la ordenación jurídica de faltas y sanciones.

FIBHULP podrá reservarse contra el trabajador las acciones civiles y/o penales que de acuerdo con la legislación vigente procedan, sin perjuicio de la sanción que pudiera imponerse en el seno de la relación laboral.

El Código Penal incluye varios tipos penales de aplicación en sus artículos 197 y siguientes, y en sus artículos 278 y 279.

En concreto, la **infracción del deber de guardar secreto profesional** puede dar lugar a las siguientes **sanciones**:

- De índole administrativa (RGPD y LOPD-GDD):
  - La normativa de protección de datos configura la vulneración del deber de secreto respecto a los datos personales como una infracción muy grave sancionada que puede conllevar una sanción de hasta 20.000.000 euros o el 4% del volumen de negocio total anual global del ejercicio anterior, según el artículo 83 del RGPD.
- De índole penal (Título X del Libro II Código Penal):
  - Prisión de 1 a 4 años y multa de 12 a 24 meses a quien, sin estar autorizado, acceda, se apodere, altere o utilice, en perjuicio de tercero, datos personales o familiares de otro, que se hallen registrados en ficheros o soportes informáticos, o de cualquier otra clase.
  - Prisión de 2 a 5 años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos.
  - Prisión de 1 a 3 años y multa de 12 a 24 meses, a quien con conocimiento de su origen ilícito pero sin haber participado en su descubrimiento, los difunda o revele.
  - Si los hechos son cometidos por la persona encargada o responsable del tratamiento, la pena de prisión será de 3 a 5 años, y si se difunden, revelan o ceden se impondrá la pena en su mitad superior.
  - Constituyen circunstancias agravantes, que supondrán la aplicación de las penas señaladas en su mitad superior, que los datos se refieran a la salud, a un menor o

incapaz o que los hechos se cometan con carácter lucrativo. Si además esta última circunstancia va referida a datos de la salud, la pena será de 4 a 6 años de prisión.

5. Descripción de las actividades de tratamiento

En el presente apartado se describen las Actividades de Tratamiento llevadas a cabo por **FIBHULP**, así como:

- los sistemas de información utilizados para llevar a cabo dichos tratamientos,
- las pautas que deben seguirse a la hora de:
    - contratar a un tercero una prestación de servicios,
    - realizar una transferencia internacional de datos fuera del Espacio Económico Europeo,
    - proporcionar un sistema de información de denuncias internas,
    - utilizar un sistema de exclusión publicitaria,
    - garantizar los derechos digitales de los trabajadores.

5.1. Registro de Actividades de Tratamiento

FIBHULP, como Responsable o Encargado del Tratamiento, llevará un Registro de las Actividades de Tratamiento efectuadas bajo su responsabilidad. Este Registro se encuentra actualmente recogido en el **Anexo I** del presente Manual de Protección de Datos.

Los Responsables Funcionales, en aquellas Actividades de Tratamiento que se les hayan encomendado, serán responsables de actualizar dicho Registro y comunicarán al Responsable del Tratamiento o al Delegado de Protección de Datos (DPO), en su caso, cualquier modificación o exclusión del mismo o la creación de una nueva actividad que implique el tratamiento de datos personales.

Este Registro deberá contener, como mínimo, para cada Actividad de Tratamiento, la siguiente información:

- Nombre y datos de contacto del Responsable del Tratamiento y, en su caso, del Corresponsable y de su representante.
- Nombre y datos del Delegado de Protección de Datos (DPO), en su caso
- Finalidades del tratamiento
- Categorías de interesados (titulares de los datos)
- Categorías de datos personales
- Categorías de destinatarios (cesiones, encargados del tratamiento, transferencias internacionales)
- Plazos de conservación de los datos personales
- Si es posible, una descripción general de las medidas técnicas y organizativas de seguridad implantadas.

La información adicional que **FIBHULP** podría incluir en el Registro de Actividades es la siguiente:

- Base legítima del tratamiento
- Origen y procedencia de los datos
- Medio de obtención / mecanismo de recogida de los datos personales
- Sistema de tratamiento
  - Aplicación o sistema informático concreto de tratamiento
  - Sistema no informatizado concreto de tratamiento
- Nombre y cargo del Responsable Funcional
- Áreas, Departamentos y/o Personas que traten o accedan a datos personales
- Procedimiento de ejercicio de derechos de protección de datos
- Datos de contacto de la persona que gestiona el ejercicio de los derechos de protección de datos
- Nivel de riesgo provisional.

5.2. Sistema de Información

La relación de **activos** (soportes automatizados, papel y otro tipo de soportes) que contienen datos personales de cada una de las Actividades de Tratamiento de FIBHULP se encuentra recogida en los Registros de Actividades de Tratamiento de la Fundación:

- Gestión de I+D+I. La Fundación, en el seno de su actividad, gestiona proyectos de investigación e innovación biomédica. En este sentido, trabaja con las personas que participan en dichos proyectos, como los investigadores, los clientes, los proveedores, los empleados y los colaboradores, tratando datos identificativos de estas personas.
- Difusión de I+D+I. La Fundación, en el seno de su actividad, se encarga de difundir información sobre los proyectos de investigación e innovación biomédica que gestiona y que lleva a cabo. En este sentido, trabaja con las personas que participan en dichos proyectos, como los investigadores, los clientes, los proveedores, los empleados y los colaboradores, tratando datos identificativos de estas personas para difundir dicha información.
- Alumnos. La Fundación gestiona cursos de formación propios y subcontratados, en este sentido, puede tratar datos de alumnos, en ocasiones como responsable del tratamiento y en ocasiones como encargado del tratamiento. Los datos que puede tratar de los

alumnos son datos identificativos, académicos y profesionales, detalles de empleo, datos económicos, y datos de transacciones de bienes y servicios.

- Ponentes. La Fundación gestiona cursos de formación propios y subcontratados, en este sentido, puede tratar datos de ponentes. Los datos que puede tratar de los ponentes son datos identificativos, académicos y profesionales, detalles de empleo, datos económicos, y datos de transacciones de bienes y servicios.
- Sugerencias y Reclamaciones. La Fundación gestiona las sugerencias y reclamaciones que los interesados introducen en un formulario de la página web de la Fundación, formulario que redirige a un correo electrónico de la Fundación. Los datos que los interesados pueden registrar en el formulario son datos identificativos, además de la sugerencia y/o reclamación en cuestión.
- Recursos Humanos. La Fundación trata los datos personales de sus empleados para gestión de nóminas, RRHH, etc.
- PRL. La Fundación únicamente trata datos relacionados con la Prevención de Riesgos Laborales para dar cumplimiento a la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- Canal de denuncias. La Fundación gestiona datos de carácter personal en los procesos de investigación de infracciones por denuncias o quejas en caso de conflicto interno y/o acoso discriminatorio, acoso moral, sexual y acoso por razón de sexo, de conformidad con el Protocolo de Prevención y Actuación ante el Acoso de la Fundación aprobado en el marco del Plan de Igualdad que lleva a cabo la Fundación.
- Proveedores. Los principales datos que trata la Fundación de este colectivo son datos de contacto, datos de detalles de empleo, datos de información comercial, datos económicos, financieros y de seguros, y datos de transacciones de bienes y servicios.
- Selección de personal. La Fundación trata datos personales de los candidatos tanto en soporte papel (curriculum vitae facilitado en mano por la persona interesada), como en soporte automatizado (a través de la plataforma Madri+d y a través del correo electrónico).
- Clientes. La Fundación trabaja únicamente con una tipología de cliente, que son los promotores (farmacéuticas, investigadores, hospitales, universidades), para gestionar los proyectos de investigación y para dar cumplimiento a obligaciones legales y contractuales.
- Investigadores. Para llevar a cabo la gestión económica de los proyectos de investigación, la Fundación requiere acceder a los siguientes datos de los investigadores: datos de carácter identificativo, características personales, datos académicos y profesionales, datos de detalles de empleo, información comercial, datos económicos, financieros y de seguros, y datos de transacciones de bienes y servicios.
- Reembolso y compensación de gastos. La Fundación, en su calidad de gestora económica, realiza el reembolso y la compensación de los gastos en los que incurren

los empleados, investigadores, pacientes, clientes y proveedores cuando participan en los proyectos de investigación. En este sentido, la Fundación, para realizar el reembolso y la compensación de gastos, únicamente accede a datos de carácter identificativo, datos de detalles de empleo, información comercial, datos económicos, financieros y de seguros, y datos de transacciones de bienes y servicios de estas personas.

- Donaciones. La Fundación trata datos de aquellas personas que realizan donaciones a FIBHULP, para lo que únicamente requiere acceder a datos de carácter identificativo y datos económicos, financieros y de seguros.
- Biobanco. La Fundación gestiona la participación de pacientes en proyectos de investigación, cuando se recogen muestras en régimen Biobanco o datos clínicos y cumplimiento de obligaciones legales y contractuales.
- Pacientes en proyectos de investigación. La Fundación trabaja con pacientes para la gestión de los proyectos de investigación cuando se recogen datos clínicos o de Resultados y Experiencias Reportados por el Paciente (Patients Reported Outcomes Management y Patient Reported Experience Management - PROMs y PREMs) en el marco de un registro, para lo que necesitan acceder a las siguientes categorías de datos de estos pacientes: datos de carácter identificativo, características personales, datos de detalles de empleo, información comercial, datos económicos, financieros y de seguros, datos de transacciones de bienes y servicios, datos de salud y datos genéticos (datos especialmente protegidos), así como datos relacionados con la recogida de PROMs y PREMs.
- Órganos de Gobierno. La Fundación únicamente trata datos de carácter identificativo de estas personas para gestionar la relación con los miembros de los Órganos de Gobierno de la Fundación y del Instituto de Investigación Sanitaria.

5.3. Encargados del Tratamiento

FIBHULP, como Responsable del Tratamiento, deberá adoptar medidas apropiadas, incluida la debida diligencia, en la elección de Encargados del Tratamiento, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme a la normativa estatal y europea vigente y, especialmente, en el RGPD, en la LOPD-GDD, así como en el presente Manual de Protección de Datos (principio de responsabilidad proactiva).

Con carácter previo a la contratación de un Encargado del Tratamiento que deba acceder a datos personales que sean responsabilidad de **FIBHULP**, así como durante la vigencia de la relación contractual, **FIBHULP** deberá verificar que el Encargado reúne las garantías necesarias y cumple con los requisitos establecidos en el RGPD en la LOPD-GDD y en el Manual de Protección de Datos.

Esta previsión se extiende también a los Encargados del Tratamiento cuando subcontraten operaciones de tratamiento con otros Subencargados. Dicha subcontratación deberá ser autorizada, por escrito, por **FIBHULP**.

Igualmente, **FIBHULP** puede actuar como prestador de servicios para diversas sociedades, sobre todo hospitales. En los contratos a firmar con estas sociedades, **FIBHULP** actuará como Encargado del Tratamiento y dichas sociedades como Responsables del Tratamiento.

Las relaciones entre Responsable y Encargado del Tratamiento, así como entre Encargado y Subencargado del Tratamiento, deben formalizarse en un **contrato** o en un acto jurídico, por escrito, inclusive en formato electrónico, que vincule al Encargado respecto al Responsable, y al Subencargado respecto al Encargado del Tratamiento, ajustado a los requisitos exigidos por la legislación aplicable, y a los establecidos en el presente Manual de Protección de Datos.

Este contrato debe establecer el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del Responsable del Tratamiento.

En concreto, este contrato estipulará que el Encargado del Tratamiento:

- tratará los datos personales únicamente siguiendo las instrucciones documentadas del Responsable del Tratamiento, salvo que esté obligado a ello en virtud de la normativa estatal o europea que se aplique al Encargado,
- garantizará que las personas autorizadas por el Encargado para tratar los datos personales se hayan comprometido a respetar la confidencialidad, o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria,
- tomará todas las medidas necesarias para garantizar la seguridad del tratamiento de datos personales,
- respetará lo dispuesto en este apartado en cuanto a la selección de Subencargados del Tratamiento,
- asistirá al Responsable del Tratamiento en el cumplimiento de atender, gestionar y dar respuesta a las solicitudes de ejercicio de derechos de protección de datos,
- ayudará al Responsable del Tratamiento a garantizar la seguridad del tratamiento de los datos personales y a realizar las consultas previas correspondientes a la Agencia Española de Protección de Datos (AEPD),

- según instrucción del Responsable del Tratamiento, suprimirá o devolverá los datos personales una vez finalice la prestación del servicio, y suprimirá cualquier copia existente, salvo que requiera la conservación de los datos por una obligación legal o para atender posibles reclamaciones de los interesados o del propio Responsable del Tratamiento,

- pondrá a disposición del Responsable del Tratamiento toda la información necesaria para demostrar el cumplimiento de lo establecido en el presente apartado,

- permitirá y contribuirá a la realización de auditorías, incluidas inspecciones, por parte del Responsable del Tratamiento o de otro auditor autorizado por el Responsable del Tratamiento,

- según instrucción del Responsable del Tratamiento, comunicará al propio Responsable del Tratamiento en un plazo inferior a las 72 horas o la Agencia Española de Protección de Datos (AEPD), en un plazo máximo de 72 horas desde que se tenga constancia de las mismas, remitiendo copia de la notificación al Responsable del Tratamiento, sobre la existencia de violaciones de la seguridad en relación con el tratamiento efectuado. Dicha notificación se realizará siguiendo el contenido mínimo requerido por el artículo 33 del RGPD,

- será considerado Responsable del Tratamiento, respecto al tratamiento de datos personales objeto del contrato, si infringe lo dispuesto en el presente apartado, en el propio contrato y, especialmente, en el RGPD y en la LOPD-GDD.

La elaboración de este contrato podrá basarse en los modelos recogidos en el **Anexos XVI** del presente Manual de Protección de Datos o en las cláusulas contractuales tipo establecidas por la Comisión Europea o la Autoridad de Control correspondiente.

La adhesión del Encargado del Tratamiento a un código de conducta o a un mecanismo de certificación, conforme al RGPD y a la LOPD-GDD, servirá para demostrar la existencia de las garantías suficientes a que se refiere este apartado.

En el **Anexo III** del presente Manual de Protección de Datos se recoge:

- el listado de Encargados del Tratamiento que prestan servicios con acceso a datos personales,

- el listado de prestadores de servicios sin acceso a datos personales, pero con libre acceso a las instalaciones de **FIBHULP**,

- el listado de Responsables del Tratamiento a los que **FIBHULP** presta algún servicio con acceso a datos personales.

5.4. Transferencias Internacionales de Datos

Todo tratamiento de datos personales que implique una transferencia de datos fuera de la Unión Europea, deberá llevarse a cabo con estricto cumplimiento de los requisitos previstos en el RGDP, en la LOPD-GDD, las disposiciones estatales y europeas aplicables y el presente Manual de Protección de Datos.

Con carácter general, no se deben transferir datos personales a países que no dispongan de la protección adecuada.

FIBHULP sólo realizará transferencias internacionales de datos personales que sean objeto de tratamiento, o vayan a serlo tras su transferencia, a un tercer país u organización internacional, si el Responsable, o en su caso, el Encargado del Tratamiento cumple con las condiciones establecidas en el RGPD y en la LOPD-GDD, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

FIBHULP solo podrá transferir datos personales a países, territorios o sectores específicos u organizaciones internacionales situados fuera de la Unión Europea, en los siguientes casos:

- **Sin necesidad de autorización específica de la AEPD:**

- Si existe, para la transferencia, una decisión de adecuación por la que la Comisión Europea reconoce que tales países, territorios, sectores u organizaciones internacionales, ofrecen un nivel de protección adecuado (Transferencias basadas en una decisión de adecuación).

- Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino (por ejemplo, en virtud de Normas Corporativas Vinculantes para Responsables y Encargados del Tratamiento, Códigos de conducta y esquemas de Certificación, así como las cláusulas contractuales tipo adoptadas por la Comisión Europea (Transferencias mediante garantías adecuadas).

- **En ausencia de una decisión de adecuación o de garantías adecuadas:**

FIBHULP solamente podrá transferir datos personales a un tercer país u organización internacional si se cumple algunas de las siguientes condiciones:

- El interesado ha dado su consentimiento explícito, tras haber sido informado de los posibles riesgos para él de dicha transferencia.

- La transferencia es necesaria para la ejecución de un contrato entre el interesado y el Responsable del Tratamiento o la ejecución de medidas precontractuales adoptadas a solicitud del interesado.

- La transferencia es necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el Responsable del Tratamiento y otra persona física o jurídica.

- La transferencia es necesaria por razones de interés público; o para la formulación, ejecución o defensa de los derechos; o para proteger intereses vitales del Interesado.

- La transferencia es necesaria para satisfacer intereses legítimos imperiosos de la Sociedad, Responsable del Tratamiento y, además, la transferencia no es repetitiva y afecta sólo a un número limitado de Interesados.

En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de los interesados y deberá comunicarse a la AEPD.

5.5. Sistemas de información de denuncias internas (Canal de Denuncias)

FIBHULP cuenta con un sistema de información de denuncias internas (Canal de Denuncias) que permita a sus empleados y a terceros denunciar, incluso anónimamente, la comisión de actos o conductas que incumplan normas generales o sectoriales, tanto por el propio personal de la empresa como por parte de terceros.

En todo momento, FIBHULP garantiza la confidencialidad de los datos personales de las personas afectadas: del denunciante, de terceros involucrados en la denuncia y, especialmente, del denunciado.

- **Deber de información**: FIBHULP informa a las partes interesadas.

- **Acceso a los datos del Canal de Denuncias**: podrán tener acceso las personas que realicen funciones de control y cumplimiento interno, los encargadas del tratamiento designados al efecto y las personas necesarias para la adopción de medidas disciplinarias (RRHH) o para la tramitación de procedimientos judiciales (Asesoría Jurídica) que, en su caso, procedan.

- **Plazo de conservación de los datos**: la información contenida en cada denuncia deberá eliminarse del sistema utilizado para interponer la denuncia cuando se haya tomado la decisión de iniciar la investigación, plazo que en ningún caso puede superar los 3 meses, salvo que se anonimice la información o sea necesario conservarla como evidencia del funcionamiento del propio sistema de información de denuncias internas. En caso de

iniciarse la investigación, los datos sólo podrán seguir siendo tratados por el órgano al que corresponda la investigación de los hechos denunciados (fuera del propio sistema utilizado para interponer la denuncia).

5.6. Envío de comunicaciones comerciales y sistemas de exclusión publicitaria

FIBHULP tiene derecho a tratar datos personales con la única finalidad de evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

- **Deber de información**: Si un interesado manifiesta su deseo de no recibir comunicación comerciales, **FIBHULP** debe darle respuesta a su solicitud conforme al procedimiento establecido en el apartado 7.7 del presente Manual de Protección de Datos (Derecho de oposición), en el que se incluirá el deber de informarle sobre los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la AEPD.

- **Deber de consulta de los sistemas de exclusión publicitaria**: En caso de realizar comunicaciones comerciales, salvo que el interesado haya dado expresamente su consentimiento para recibir dicho tipo de comunicaciones, **FIBHULP** deberá consultar previamente los sistemas de exclusión publicitaria que pudieran afectar a su actuación (y que estén incluidos en la relación publicada por la AEPD), excluyendo, de esta actividad de tratamiento de envíos de comunicaciones comerciales, los datos personales de las personas que hubieran manifestado su oposición.

5.7. Derechos Digitales de los trabajadores

De acuerdo con el art. 20 bis ET, los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por **FIBHULP**, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia, grabación de sonidos y geolocalización.

La entidad deberá poner en marcha una **Política Interna de Garantía de los Derechos Digitales** que contenga, como mínimo:

- Criterios de utilización de los dispositivos digitales puestos a su disposición por la entidad.

- Usos autorizados y, en su caso, periodos en los que estos dispositivos digitales podrán ser utilizados para fines privados.

- Garantías para preservar la intimidad de los trabajadores.

- Modalidades de ejercicio del derecho a la desconexión digital.

- Acciones de formación y de sensibilización del personal sobre el uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática.

En caso de que la entidad haya implantado sistemas de videovigilancia, grabación de sonidos y/o geolocalización:

- Informar previamente a los trabajadores sobre la implantación de sistemas de videovigilancia, grabación de sonidos y/o geolocalización, características de los mismos

- Informar previamente acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

En el **Anexo XXI** del presente Manual de Protección de Datos se recoge un modelo de **Política Interna de Garantía de los Derechos Digitales**.

5.7.1 Dispositivos digitales

- **Deber de información**: **FIBHULP** deberá informar a los trabajadores sobre los criterios de uso de los dispositivos digitales puestos a su disposición para desarrollar su trabajo, de acuerdo con lo establecido al respecto en el apartado 4.4.5 del presente Manual de Protección de Datos ("Funciones y Obligaciones del personal con acceso a datos) y en la Política Interna de Garantía de los Derechos Digitales, recogida en el **Anexo XXI** del presente Manual de Protección de Datos.

5.7.2 Desconexión digital

- **Deber de información**: **FIBHULP** informará a los trabajadores sobre su derecho a la desconexión digital en el ámbito laboral a través de una política interna que defina las modalidades de ejercicio de este derecho. Esta política está contenida en la Política Interna de Garantía de los Derechos Digitales, recogida en el **Anexo XXI** del presente Manual de Protección de Datos.

5.7.3 Dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo

- **Ubicación de las cámaras**: Respetando en todo momento la intimidad de los trabajadores, **FIBHULP** no instalará, bajo ninguna circunstancias, cámaras de videovigilancia y/o de grabación de sonidos en zonas destinadas al descanso o esparcimiento de los trabajadores, ni en vestuarios, aseos, comedores o zonas análogas.

- **Ubicación de los sistemas**: Los monitores donde se visualicen las imágenes de las cámaras, así como los sistemas de reproducción de la grabación de sonidos se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.

- **Conservación de imágenes y de sonidos**: Las imágenes y sonidos se almacenarán durante el plazo máximo de un mes, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes y sonidos deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

- **Deber de información**: Se informará acerca de la existencia de los sistemas de grabación de imágenes y/o sonidos mediante un distintivo informativo donde mediante un pictograma y un texto (**Anexo XV**) se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo.

- **Control laboral**: Cuando las imágenes y/o sonidos vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes y/ sonidos captados por las cámaras y/o los sistemas de grabación de sonidos.

- **Derecho de acceso a las imágenes y a los sonidos**: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el DNI del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.

- **No se facilitará al interesado acceso directo a las imágenes y sonidos en las que se muestren imágenes o sonidos de terceros.** En caso de no ser posible la visualización de las imágenes o la escucha de los sonidos por el interesado sin mostrar imágenes o sonidos de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes o sonidos del interesado.

5.7.4 Sistemas de geolocalización en el ámbito laboral

Derecho de información: Respetando en todo momento la intimidad de los trabajadores, **FIBHULP** no instalará, bajo ninguna circunstancias, sistemas de geolocalización sin informar previamente, de forma expresa, clara e inequívoca, a los trabajadores de la existencia y características de los dispositivos de geolocalización. Igualmente deberá informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

6. Procedimientos de Protección de Datos

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, **FIBHULP**, como Responsable y/o Encargado del Tratamiento, **debe decidir qué medidas de seguridad, técnicas y organizativas, implantar para garantizar un nivel de seguridad adecuado al riesgo**. Dichas medidas pueden incluir, entre otros:

- la seudonimización y el cifrado de los datos personales,
- la capacidad de garantizar la confidencialidad, la integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento,
- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico,
- las medidas de seguridad adicionales que, en su caso, vengan exigidas por la legislación estatal o europea aplicable a Responsables y Encargados del Tratamiento,
- el proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento,
- la adhesión a un código de conducta o a un mecanismo de certificación, aprobados conforme a la legislación aplicable, ya que pueden servir como medio de prueba del cumplimiento de los requisitos de seguridad.

No obstante, FIBHULP estará sujeto al cumplimiento del Esquema Nacional de Seguridad (ENS) en caso de tratarse de una Administración Pública, de una de las entidades enumeradas en el art. 77 de la LOPD-GDD o de prestar un servicio en régimen de concesión, encomienda de gestión o contrato, a una Administración Pública.

6.1. Medidas de Seguridad a aplicar a tratamientos automatizados

En este apartado se recogen las medidas de seguridad, relacionadas con tratamientos automatizados, que FIBHULP, como Responsable o Encargado del Tratamiento, ha decidido implantar para proteger los datos personales, así como para garantizar y poder demostrar el cumplimiento del RGPD y de la LOPD-GDD (principio de responsabilidad proactiva).

Las medidas de seguridad implantadas serán revisadas de forma periódica con el objetivo de comprobar que garantizan un nivel de seguridad adecuado al riesgo, que protegen efectivamente la seguridad de los datos personales y que permiten demostrar el cumplimiento del RGPD y de la LOPD-GDD.Ordenadores y dispositivos

6.1.1 Ordenadores y dispositivos

- **Actualización**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible. Los Sistemas Operativos utilizados en los equipos informáticos de la Fundación son los siguientes: Windows 8.1 (32 bits), Windows 7 y Windows 10. Así mismo, la Fundación cuenta con una Red LAN segmentada por VLANs desde 10.35.16.0 a 10.35.32.254 (IP fijos), y desde 10.133.10 a 10.133.32.254 (HCP).

- **Antivirus**: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida de lo posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica. La Fundación tiene instalado, configurado y actualizado en todos los equipos informáticos el antivirus Panda.

- **Firewall**: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales. Como medidas de seguridad, la Fundación dispone de un Firewall Bitdefender, así como una Sonda Parimetral (OSI) que detecta posibles problemas en los sistemas de información.

6.1.2 Control de acceso físico

El acceso a datos personales queda absolutamente restringido a las personas autorizadas en el **Anexo II** del presente Manual de Protección de Datos.

- **Control de accesos**: La autorización de los usuarios para acceder a los locales donde se encuentren ubicados los sistemas de información, así como a los propios sistemas, equipos, aplicaciones y, en general, a datos personales, dependerá de las funciones que desarrollen en cada momento. Los usuarios solo tendrán acceso a aquellos datos estrictamente necesarios para el desarrollo de las funciones que la Fundación les haya encomendado. El Responsable Funcional podrá conceder, alterar o anular el acceso autorizado del personal sobre los datos y recursos, de conformidad a las necesidades inherentes a su puesto de trabajo. Los sistemas informáticos de la Fundación que contienen datos de carácter personal tienen restringido su acceso mediante un código de usuario y una contraseña, así mismo, al servidor donde se conservan los datos responsabilidad de la Fundación únicamente se puede acceder con usuario y contraseña. Se trata de un servidor NTFS al que se accede por

permisos de usuario para lectura, escritura, modificación y borrado. Hay dos niveles de permisos, uno para el acceso a las carpetas donde se almacena la información y otro permiso para el acceso a las subcarpetas. A estas carpetas únicamente podrán acceder empleados de la Fundación.

6.1.3 Control de acceso lógico

Un objetivo prioritario para la normativa aplicable en materia de protección de datos es evitar cualquier tipo de uso indebido o no autorizado a datos personales. Por ello, se deben implantar una serie de procedimientos de identificación y autenticación que permitan obtener y verificar puntualmente la identidad del usuario de forma inequívoca.

- 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.
- 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 para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
- 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, no se dejarán anotadas en lugar común, ni se permitirá el acceso de personas distintas del usuario.
- Previamente a la asignación de nombres de usuario y contraseña, se definirán las pantallas, módulos y procesos a los que tendrán acceso autorizado cada uno de los usuarios que prestan servicios para la Fundación.
- Todas las aplicaciones estándar bajo Sistema Operativo, hojas de cálculo, bases de datos, documentos de texto, etc., que contengan datos personales, se configurarán de tal modo que al ejecutarse alguna de ellas se deba introducir una contraseña. Se exceptuará esta obligación en caso de existencia de aplicativos de gestión de identidades o Single Sign On.
- Igualmente, las aplicaciones a medida o de terceros también deberán configurarse de modo que los usuarios deban introducir una contraseña.
- Se limitará el número de intentos de acceso tanto al Sistema Operativo como a las aplicaciones a medida o de terceros, de forma que tras tres intentos fallidos, se

inhabilitaría el acceso del usuario de forma permanente, hasta que el administrador vuelva a permitir el acceso.
- Las contraseñas deben cambiarse periódicamente, preferiblemente cada 2 ó 3 meses.
- Las contraseñas deben almacenarse de forma cifrada, de forma que únicamente los usuarios conozcan sus propias contraseñas.

En este sentido, la Fundación dispone de contraseñas de acceso a los sistemas de información individuales, las cuales constan de ocho caracteres alfanuméricos, combinando letras mayúsculas y minúsculas. Así mismo, el acceso a la aplicación informática Fundanet, se bloquea al quinto intento de acceso no autorizado.

Recomendaciones a los usuarios para elegir su contraseña:

Cada usuario es responsable de la confidencialidad de su contraseña, por lo que si advierte o sospecha que la misma ha podido ser conocida fortuita o fraudulentamente por personas no autorizadas, deberá cambiarla inmediatamente y notificarlo como incidencia al Responsable de Seguridad Técnico, el cual podrá asignar una nueva contraseña al usuario si dicho usuario no supiera cambiar la misma por sí mismo o, incluso, bloquear la cuenta del usuario si hiciera falta.

Se establecen a continuación una serie de recomendaciones o consejos, en orden a garantizar la seguridad de las contraseñas en su construcción y gestión:

- No dejar espacios en blanco en la contraseña.
- No dejar la contraseña en blanco.
- Longitud mínima de 10 caracteres alfanuméricos (letras + al menos 1 número), combinando también letras mayúsculas y minúsculas.
- No contener el nombre de usuario como parte de la contraseña.
- Introducir una contraseña fácil de recordar, de modo que no sea necesario que se anote en ningún lugar cercano, pero difícil de adivinar.
- No usar palabras reconocibles del diccionario y en especial palabras asociadas al usuario concreto: el nombre de cónyuges y parientes, amigos, mascotas o pueblos, sus fechas de nacimiento, meses o días de la semana, empresa para la que trabaja, números de matrícula o teléfonos, palabras comunes de otros idiomas y secuencias de caracteres del teclado de un ordenador.
- No dejarla por escrito, para que no sea visible para otros usuarios.
- No compartirla con otros usuarios.
- No utilizar contraseñas iguales para temas personales que para temas profesionales.
- Cambiarla periódicamente (ya le obligue el sistema a hacerlo o no).
- No repetir las últimas 3 contraseñas utilizadas.

- Cambiar la contraseña que se le haya asignado temporalmente una vez que sea utilizada por primera vez.

- **Registro de accesos**: se debe valorar la existencia de este registro de accesos, especialmente si se trata de **datos sensibles**. Estos accesos pueden ser controlados a través de una aplicación de gestión de identidades. En los casos en que acceda más de un usuario a los datos personales, se guardará un registro de cada acceso en el que conste la identificación del usuario, la fecha y hora del acceso, los datos a los que accede, el tipo de acceso y si fue autorizado o denegado. Si el acceso se autoriza, se guardará además la información que permita identificar el registro accedido y, si es posible, qué acción ha realizado, durante, al menos, dos años. El **Responsable de Seguridad Técnico** revisará periódicamente la información registrada. En la Fundación se controla qué usuario ha modificado cada uno de los documentos.

6.1.4 Gestión de soportes

Todos los soportes que contengan datos personales deben estar identificados, etiquetados, inventariados y almacenados en un lugar con acceso restringido. En el **Anexo V** del presente Manual de Protección de Datos se recoge el Inventario de Soportes.

- **Control de entrada y salida de soportes**: el **Responsable Funcional** de cada Actividad de Tratamiento, deberá autorizar la entrada y salida de soportes con datos personales fuera de los locales en los que están ubicados, y llevar un Registro en el que conste el tipo y cantidad de soportes que entran o salen; la referencia genérica del tipo de datos contenidos; la fecha y hora de salida o entrada; la forma de envío o recepción; y la identificación detallada de los datos del receptor, o en su caso emisor. Los **Anexos VI y VII** del presente Manual de Protección de Datos recogen estos Registros de entrada y salida de soportes.

- **Reutilización y destrucción de soportes**: cuando un soporte con datos personales vaya a ser reutilizado o destruido, previamente deberá ser borrada toda la información que contiene mediante un sistema que no permita su aprovechamiento posterior. En el primer caso, se procederá al borrado lógico de la información de los soportes, de tal forma que no se permita el recuperado de la información. En el segundo caso, se procederá además a la destrucción completa del soporte.

- **Distribución de soportes**: en caso de producirse una salida de soportes con datos personales fuera de los sistemas de información de la Fundación, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información, especialmente si se trata de **datos sensibles**.

6.1.5 Gestión de incidencias

Las incidencias de seguridad serán notificadas, registradas y gestionadas para asegurar que se toman las medidas adecuadas para su resolución.

Todo aquello acontecido que se considere una incidencia debe quedar debidamente reflejado en un Registro habilitado al efecto. De las incidencias resueltas se dejará constancia en el Registro de Incidencias, en el que deberá constar, como mínimo, la siguiente información:

- Tipo de incidencia
- Fecha y hora en que se produjo
- Persona que realiza la notificación
- Persona a quien se comunica
- Efectos que puede producir
- Descripción detallada de la misma

En los casos en los que sea necesario proceder a la recuperación de datos para subsanar la incidencia, además se harán constar los siguientes datos:

- Autorización del Responsable de Seguridad
- Procedimientos realizados
- Persona que realizó el proceso
- Datos restaurados
- Datos grabados manualmente

El Responsable Funcional deberá asegurarse de que los técnicos den respuesta a la incidencia detectada y supervisará el trabajo de subsanación de la misma. Cualquier usuario que tenga conocimiento de una incidencia deberá notificarlo al Responsable de Seguridad Técnico. Dicha comunicación deberá realizarse a la mayor brevedad posible desde que se produzca o se tenga conocimiento de dicha incidencia. El conocimiento de una incidencia, por parte de un usuario, y su falta de notificación a la persona o personas encargadas de recibir las mismas se considerará como una falta grave contra la seguridad de los datos por parte de dicho usuario. Todas las incidencias ocurridas se mantendrán registradas durante, al menos, un período de doce (12) meses.

Este procedimiento de incidencias deberá ser conocido por todos los empleados y colaboradores de **FIBHULP**, que por sus funciones en la misma, traten datos personales. Dicho plan consta de tres fases:

- **Notificación**: Cualquier persona que preste servicios para **FIBHULP** y detecte alguna anomalía en los sistemas, soportes o equipos informáticos, o en los datos personales contenidos en los mismos, deberá ponerlo en conocimiento inmediato del **Responsable de Seguridad Técnico**. De esta forma tratará de evitarse que la posible incidencia repercuta negativamente en la seguridad con la que son tratados y mantenidos los datos personales. Esta comunicación con el **Responsable de Seguridad Técnico** debe realizarse a través

del medio más rápido y fiable posible para que se mantenga la seguridad y confidencialidad de los datos personales. La persona que se ponga en contacto con el **Responsable de Seguridad Técnico** a fin de notificarle la incidencia, debe facilitarle la información necesaria para que se proceda a su registro y control, así como para poner en marcha, si fuera posible, un plan de respuesta para interrumpir y eliminar la incidencia.

- **Registro**: El **Responsable de Seguridad Técnico** cuenta con una hoja Registro de incidencias, cuyo modelo se adjunta como **Anexo IV**, en la que se deben hacer constar los datos relativos a las incidencias ocurridas. Esta hoja debe estar perfectamente cumplimentada, haciendo constar en ella con exactitud cada uno de los datos que en la misma se requieren. Es competencia exclusiva del **Responsable de Seguridad Técnico**, el mantenimiento y cumplimiento de las medidas adoptadas para atender las posibles incidencias. Con ese objeto, llevará un registro de incidencias en el que constarán todos los aspectos relativos a la incidencia acaecida.

- **Gestión**: El **Responsable de Seguridad Técnico** comunicará la incidencia a los técnicos internos o externos que se ocupan de la seguridad y mantenimiento de los sistemas, equipos y aplicaciones que contengan datos personales. El **Responsable de Seguridad Técnico** se asegurará que, a la mayor brevedad posible, los técnicos den respuesta a las incidencias detectadas y supervisará personalmente la actividad de los mismos y la subsanación de la anomalía. El **Responsable de Seguridad Técnico** comunicará a **FIBHULP** las incidencias que puedan afectar gravemente los derechos y libertades de los individuos. Finalizada la incidencia, el **Responsable de Seguridad Técnico** adoptará las medidas necesarias para que no vuelva a producirse una situación similar en la que pueda peligrar la integridad de los sistemas, equipos y aplicaciones que contengan datos personales.

La Fundación cuenta con Registro de Incidencias en su Intraweb, registro que gestiona directamente la Comunidad de Madrid.

6.1.6 Copias de seguridad

La posibilidad de que en una incidencia puedan perderse datos personales que constan en los sistemas informáticos de **FIBHULP**, obliga a que se conserven copias de seguridad de todos los archivos, programas, etc., que contengan datos personales.

Todo programa, aplicación o base de datos utilizado para el tratamiento de datos personales deberá proveer la función de realización de copias de seguridad, o bien, permitir la realización de copias de seguridad de tal forma que se garantice la recuperación de datos.

Periódicamente, como mínimo una vez a la semana, 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 ordenador o servidor con los archivos, programas, etc., originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Antes de proceder al almacenamiento de la copia de seguridad se verificará que ésta se ha realizado correctamente y sin ninguna incidencia.

Las recuperaciones de datos personales requieren la autorización del **Responsable Funcional** correspondiente.

Se realizarán pruebas cada 6 meses que verifiquen la disponibilidad efectiva de los datos contenidos en los dispositivos de copias de seguridad.

Este procedimiento deberá ser comunicado de forma clara y legible al personal a quien haya sido encomendada dicha función de forma expresa, quien queda obligado a:

- La realización de las copias de seguridad y la conservación de las mismas conforme a lo establecido en el presente apartado.

- Deber de confidencialidad sobre el modo o sistema de realización de las mencionadas copias, salvo a las personas autorizadas.

- Prohibición de entregar las copias de seguridad a persona distinta de aquellas que hayan sido debidamente autorizadas.

- Prohibición de manipular, alterar o deteriorar los soportes (cintas, disquetes, etc.) en los que se realizan las copias de seguridad.

En la Fundación se realiza un back up mensual (se guardan las copias de seguridad de los últimos cuatro meses) dos veces al día. Así mismo, cada año se realiza una copia que hace desaparecer la copia del año anterior.

6.1.7 Pruebas con datos reales

Con el fin de que la seguridad de los datos personales se encuentre garantizada, se realizarán pruebas con carácter previo a la implantación o modificación de los sistemas de información que traten datos personales.

Las pruebas anteriores a la implantación de las medidas de seguridad no se realizarán en ningún caso con datos reales.

Únicamente cuando se garantice un nivel de seguridad adecuado, podrán utilizarse datos reales en la realización de las mismas.

El **Responsable de Seguridad Técnico** está obligado a comprobar el cumplimiento de la presente medida de seguridad.

6.1.8 Seudonimización

Siempre que sea posible, se procurará reducir la trazabilidad entre la información tratada y la identidad del interesado cuyos datos se están tratando, de forma que se reduzcan los riesgos derivados del tratamiento de datos personales.

6.1.9 Cifrado

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 deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información, especialmente si se trata de **datos sensibles**.

Actualmente en la Fundación existe un acceso seguro a través de VPN (con usuario y contraseña) para el acceso remoto a los sistemas desde fuera de las instalaciones de la Fundación. Este acceso únicamente está permitido para usuarios VIP, y para proveedores e informáticos que requieran dar soporte externo a la Fundación.

6.1.10 Plan de Contingencias

Para el supuesto en el que se produzca una pérdida total y absoluta de datos o que los sistemas sean destruidos total o parcialmente por cualquier contingencia imposible de prever, se deberá proceder de la siguiente forma:

- Organizar y estructurar el sistema informático en otro Centro o Dependencia que posea la Fundación; o bien acudir al alquiler de oficinas donde instalar la unidad del Servidor Central o de los sistemas de tratamiento.

- Recurrir a una copia de seguridad de todos los programas, aplicaciones o bases de datos, con la cual la Fundación podrá poner en marcha, de forma inmediata, su actividad.

6.2. Medidas de Seguridad a aplicar a tratamiento no automatizados

En este apartado se recogen las medidas de seguridad, relacionadas con tratamientos no automatizados, que FIBHULP, como Responsable o Encargado del Tratamiento, ha decido implantar para proteger los datos personales, así como para garantizar y poder demostrar el cumplimiento del RGPD y de la LOPD-GDD (principio de responsabilidad proactiva).

Las medidas de seguridad implantadas serán revisadas de forma periódica con el objetivo de comprobar que garantizan un nivel de seguridad adecuado al riesgo, que protegen efectivamente la seguridad de los datos personales y que permiten demostrar el cumplimiento del RGPD y de la LOPD-GDD.

6.2.1 Control de acceso físico

El acceso a los locales donde se encuentren ubicados los soportes no automatizados con datos personales y el acceso a los propios datos personales queda absolutamente restringido a las personas autorizadas en el **Anexo II** del presente Manual de Protección de Datos.

La presencia de terceros en los citados locales sólo podrá tener lugar cuando se encuentren acompañados de un usuario autorizado, bajo la completa responsabilidad de éste y con la autorización expresa del **Responsable de Seguridad Técnico** o del **Responsable Funcional** correspondiente. En ningún caso la presencia de terceros podrá suponer que estos accedan a los sistemas de información o a datos personales.

Por ello, únicamente las personas autorizadas, dependiendo de las funciones que desarrollen en cada momento, podrán tener acceso a la información en soporte papel. Los usuarios solo tendrán acceso a aquellos datos estrictamente necesarios para el desarrollo de las funciones que la Fundación les haya encomendado.

En caso de acceder a **datos sensibles**, se deberá identificar al usuario con acceso a este tipo de tratamiento, la Actividad de Tratamiento correspondiente, la fecha y hora del acceso, y la documentación o datos a los que tiene acceso. El **Anexo VII** del presente Manual de Protección de Datos contiene una plantilla de Registro de Accesos. El acceso realizado a esta documentación por personas no autorizadas también deberá anotarse en dicho Registro.

Actualmente, en la Fundación, existe un Control de acceso físico al CPD. Al CPD se accede con tarjeta, a la sala de operadores del CPD tiene acceso toda la plantilla de informática. No obstante, al CPD principal únicamente tiene acceso el jefe de servicio, el administrador y dos operadores. En caso de que al CPD vaya a acceder un tercero externo al departamento de informática, el tercero deberá rellenar un documento (Protocolo de Acceso al CPD) que contiene la siguiente información: número de orden, nombre y apellidos, NIF, empresa, entrada (fecha y hora), firma de la entrada, motivo de la visita, quién ha autorizado el acceso, salida (fecha y hora), y firma de la salida. Así mismo, estas personas externas, siempre deberán acceder acompañados de alguna de las personas con autorización para acceso al CPD principal. El CPD cuenta con la siguiente seguridad física: 4 máquinas de aire, temperatura de 15 grados y humedad del 50%. Así mismo, todos los servidores están en RAR.

6.2.2 Gestión de incidencias

Las incidencias de seguridad a datos personales en soportes no automatizados serán notificadas, registradas y gestionadas, para asegurar que se toman las medidas adecuadas para su resolución, de la misma manera que para los datos automatizados. El **Anexo IV** del presente Manual de Protección de Datos recoge la plantilla para el registro de incidencias que afecten a datos personales.

Este procedimiento de incidencias deberá ser conocido por todos los empleados y colaboradores de **FIBHULP**, que por sus funciones en la misma, traten datos personales. Dicho plan consta de tres fases:

- **Notificación**: Cualquier persona que preste servicios para **FIBHULP** y detecte alguna anomalía en los datos personales contenidos en soportes no automatizados, deberá ponerlo en conocimiento inmediato del **Responsable Funcional** de la correspondiente Actividad de Tratamiento afectada. De esta forma tratará de evitarse que la posible incidencia repercuta negativamente en la seguridad con la que son tratados y mantenidos los datos personales. Esta comunicación con el **Responsable Funcional** correspondiente debe realizarse a través del medio más rápido y fiable posible para que se mantenga la seguridad y confidencialidad de los datos personales. La persona que se ponga en contacto con el **Responsable Funcional** correspondiente a fin de notificarle la incidencia, debe facilitarle la información necesaria para que se proceda a su registro y control, así como para poner en marcha, si fuera posible, un plan de respuesta para interrumpir y eliminar la incidencia.

- **Registro**: El **Responsable Funcional** correspondiente cuenta con una hoja Registro de incidencias, cuyo modelo se adjunta como **Anexo IV**, donde debe hacer constar los datos relativos a las incidencias ocurridas. Deben estar perfectamente cumplimentados, haciendo constar en ella con exactitud cada uno de los datos que en la misma se requieren. Es competencia exclusiva del **Responsable Funcional** correspondiente, el mantenimiento y cumplimiento de las medidas adoptadas para atender las posibles incidencias. Con ese objeto, llevará un registro de incidencias en el que constarán todos los aspectos relativos a la incidencia acaecida.

- **Gestión**: El **Responsable Funcional** correspondiente comunicará la incidencia a su personal, se asegurará que, a la mayor brevedad posible, se dé una respuesta a las incidencias detectadas y supervisará personalmente la subsanación de la anomalía. El **Responsable Funcional** correspondiente comunicará al Delegado de Protección de Datos (DPO) las incidencias que puedan afectar a los derechos y libertades de los individuos. Finalizada la incidencia, el **Responsable Funcional** correspondiente adoptará las medidas

necesarias para que no vuelva a producirse una situación similar en la que pueda peligrar la integridad de los datos personales en soporte no automatizado.

6.2.3 Gestión de soportes

Los soportes extraíbles y los documentos en papel serán identificados, etiquetados, inventariados y almacenados en armarios u otro tipo de mobiliario con sistemas de cierre, de forma que se obstaculice su apertura.

En caso de que esto no sea posible, deben adoptarse las medidas necesarias para impedir el acceso a la documentación en papel por personas no autorizadas.

Mientras la documentación con datos personales no se encuentre archivada en los dispositivos de almacenamiento establecido en el punto anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

La documentación que contenga **datos sensibles** se almacenará en locales con sistemas de cierre y permanecerán cerrados cuando no sea preciso el acceso a esta documentación.
Siempre que se proceda al traslado físico de la documentación con **datos sensibles**, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Los soportes que contengan datos personales y la documentación en papel debe eliminarse de forma segura cuando ya no sea necesario su tratamiento y hayan pasado los plazos de conservación. Para garantizar su destrucción, FIBHULP:

- Subcontratará a una empresa especializada en destrucción de soportes y papel
- Triturará el papel con una destructora de papel
- Destruirá físicamente el soporte asegurando la no recuperación de la información que contiene

6.2.4 Copias o reproducción de documentos con datos sensibles

Las copias o reproducciones de documentos con datos sensibles deberá ser controlada y debidamente autorizada.

Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

6.2.5 Seudonimización

Siempre que sea posible, se procurará reducir la trazabilidad entre la información tratada y la identidad del interesado cuyos datos se están tratando, de forma que se reduzcan los riesgos derivados del tratamiento de los datos personales.

6.3. Controles de verificación de cumplimiento

Los Responsables Funcionales y el Responsable de Seguridad Técnico, con el asesoramiento del Delegado de Protección de Datos (DPO) revisarán **periódicamente** el cumplimiento de los dispuesto en el presente Manual de Protección de Datos y en la normativa estatal y europea vigente de protección de datos, especialmente en el RGPD y en la LOPD-GDD.

Las plantillas de Registro de Controles Periódicos tanto para soportes automatizados como no automatizados se recogen en el **Anexo VIII** del presente Manual de Protección de Datos.

6.4. Procedimiento de notificación de brechas de seguridad

Se considera violación, quiebra o brecha de seguridad a toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

El procedimiento de gestión y notificación de brechas de seguridad se encuentra recogido en **Anexo XVII** del presente Manual de Protección de Datos.

6.5. Procedimiento para llevar a cabo una Evaluación de Impacto (EIPD)

El procedimiento para llevar a cabo una Evaluación de Impacto relativa a la Protección de Datos (EIPD) se encuentra recogido en Anexo XX del presente Manual de Protección de Datos.

7. Derechos de protección de datos

7.1. Derecho de información

Según el principio de transparencia, principio vinculado al derecho de información, **FIBHULP**, como Responsable del Tratamiento, debe informar a los interesados sobre el tratamiento que va a realizar de sus datos. Esta información debe facilitarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, por escrito o por otros medios, incluso por medios electrónicos.

FIBHULP no debe recabar ni tratar datos personales relativos al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física, salvo que la recogida de dichos datos sea consentida explícitamente por el propio interesado, o sea necesaria, por ejemplo, para proteger el interés vital del interesado o por razones interés público en salud pública, para la atención de reclamaciones, para fines de medicina preventiva o laboral, o requerida o autorizada por la legislación estatal o europea aplicable, en cuyo caso será recabado y tratado de acuerdo con lo establecido en la misma.

En los procesos de recogida y obtención de datos personales, **FIBHULP** debe informar a los interesados, principalmente, de la identidad del Responsable del Tratamiento y del Delegado de Protección de Datos (DPO), los fines del tratamiento, la base legítima del tratamiento, los destinatarios de los datos, su plazo de conservación, sus derechos de protección de datos.

El presente Manual de Protección de Datos recoge, en el **Anexo XV**, las cláusulas a utilizar para informar a los interesados sobre estos aspectos.

En estas cláusulas se informa a los interesados sobre el ejercicio de sus derechos, y en concreto, de sus derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición, así como sobre la forma para ejercerlos, que debe ser visible, accesible y sencilla.

FIBHULP posibilitará la presentación de solicitudes por medios electrónicos, especialmente cuando la recogida de los datos y el tratamiento de los mismos se realizan por estos medios. Igualmente, deberá darse respuesta por medios electrónicos si la solicitud es realizada a través de dichos medios, salvo que el interesado manifieste lo contrario.

Los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición son derechos independientes, de manera que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro; asimismo, su ejercicio tampoco puede dar lugar a la exigencia de contraprestación alguna, sea de tipo económico o no.

Al encontrarnos ante derechos personalísimos, deberán ser ejercitados por el titular de los datos frente al responsable del tratamiento. No obstante, podrá actuar su representante legal cuando el titular se encuentre en situación de discapacidad o minoría de edad que le imposibilite el ejercicio personal de los derechos.

FIBHULP ha acordado la designación del siguiente **Gestor de solicitudes de ejercicio de derechos,** encargado de gestionar y contestar en plazo dichas solicitudes, de acuerdo al procedimiento establecido en el presente apartado.

Gestor de solicitudes de ejercicio de derechos: Sara Fernández

FIBHULP, ante una solicitud de ejercicio de un derecho de protección de datos, deberá responder al interesado en el **plazo de un mes** a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes, informando de ellos al interesado en el mismo plazo de un mes indicando los motivos de la dilación.

La información facilitada a los interesados y cualquier comunicación o actuación realizada en virtud del ejercicio de un derecho de protección de datos debe ser gratuito, salvo que las solicitudes sean manifiestamente infundadas o excesivas, especialmente por ser repetitivas (**menos de 6 meses**), en cuyo caso **FIBHULP** podrá cobrar un canon razonable o negarse a atender dicha solicitud.

7.2. Derecho de acceso

Los interesados pueden obtener del Responsable del Tratamiento confirmación de si se están tratando o no datos personales que le conciernen, junto con información referente a los fines del tratamiento, las categorías de datos personales que se traten, los destinatarios o categorías de destinatarios a los que se comunicaron los datos, las garantías adecuadas relativas a transferencias internacionales de datos, el plazo de conservación, la posibilidad de ejercer sus derechos en protección de datos, así como de presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD) o Autoridad de Control correspondiente, el origen de los datos (si no han sido obtenidos del propio interesado) y de la existencia de decisiones individuales automatizadas, incluida la elaboración de perfiles.

FIBHULP facilitará al interesado una copia de los datos personales objeto del tratamiento y podrá cobrar un canon si el interesado solicita cualquier otra copia.

Para la puesta en práctica de este derecho, **FIBHULP** deberá tener en cuenta todo lo que se detalla a continuación:

- Para ejercitar el derecho de acceso, al igual que el resto de derechos de protección de datos, el titular de los datos deberá dirigir a la Fundación una solicitud que contenga su nombre y apellidos y fotocopia de su DNI (o acreditación de su identidad por cualquier otro medio válido en derecho) o persona que lo representa, así como el documento acreditativo de tal representación; petición en que se concreta la solicitud; domicilio a efectos de notificaciones y fecha y firma del solicitante. Se recoge modelo de solicitud en el **Anexo XII** del presente Manual de Protección de Datos.

- Si la solicitud no reúne los requisitos recogidos en el primer punto, la Fundación debe solicitar su subsanación.
- La Fundación debe contestar la solicitud, utilizando cualquier medio que permita acreditar su envío y recepción. La solicitud deberá ser resuelta en el **plazo de un mes** a contar desde su recepción.
- Si la resolución fuera estimatoria, se debe hacer efectivo el acceso a los datos. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación positiva al ejercicio de derechos.
- El ejercicio del derecho de acceso podrá ser denegado cuando ya se haya ejercitado este derecho en un intervalo inferior a **6 meses** y el interesado no acredite un interés legítimo o cuando exista una obligación legal que impida la revelación de dichos datos. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación negativa al ejercicio de derechos.
- En el caso de que no se dispongan de datos personales del interesado, se deberá igualmente comunicar en el mismo plazo.
- Se debe informar al interesado de su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD) o Autoridad de Control correspondiente, así como la posibilidad de ejercer ante el Responsable del Tratamiento cualquier otro derecho de protección de datos.

7.3. Derecho de rectificación

Los interesados pueden solicitar a **FIBHULP** que, sin dilación indebida, rectifique los datos inexactos que le conciernan o se completen los datos personales que sean incompletos.

- Para ejercitar el derecho de rectificación, el titular de los datos deberá dirigir a la Fundación una solicitud que contenga su nombre y apellidos y fotocopia de su DNI (o acreditación de su identidad por cualquier otro medio válido en derecho) o persona que lo representa, así como el documento acreditativo de tal representación; petición en que se concreta la solicitud; domicilio a efectos de notificaciones y fecha y firma del solicitante. Se recoge modelo de solicitud en el **Anexo XII** del presente Manual de Protección de Datos.
- En la solicitud, el interesado deberá indicar, además, el dato erróneo y la corrección que debe realizarse.
- Si la solicitud no reúne los requisitos recogidos en los puntos anteriores, la Fundación debe solicitar su subsanación.

- La Fundación debe contestar la solicitud, utilizando cualquier medio que permita acreditar su envío y recepción.
- La solicitud deberá ser resuelta en el **plazo de un mes** a contar desde su recepción.
- Si la resolución fuera estimatoria, se debe hacer efectiva la rectificación de los datos. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación positiva al ejercicio de derechos.
- El ejercicio del derecho de rectificación podrá ser denegado cuando ya se haya ejercitado este derecho en un intervalo inferior a **6 meses** y el interesado no acredite un interés legítimo o cuando pudiese causar un perjuicio a intereses legítimos, tanto del titular de los datos como de terceros o cuando exista una obligación legal de conservación de datos. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación negativa al ejercicio de derechos.
- En el caso de que no se dispongan de datos personales del interesado, se deberá igualmente comunicar en el mismo plazo.
- Se debe informar al interesado de su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD) o Autoridad de Control correspondiente, así como la posibilidad de ejercer ante el Responsable del Tratamiento cualquier otro derecho de protección de datos.
- En los casos en los que los datos rectificados hayan sido comunicados a terceras personas y se mantenga el tratamiento por éstas, la Fundación deberá comunicarles la rectificación para que ellas también la efectúen.

7.4. Derecho de supresión y derecho al olvido

Los interesados pueden solicitar a **FIBHULP** que, sin dilación indebida, suprima sus datos personales y deje de tratarlos, si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si han retirado su consentimiento o se oponen al tratamiento de sus datos personales, o si dicho tratamiento es ilícito o incumple de otro modo el RGPD y la LOPD-GDD.

- Para ejercitar el derecho de supresión, el titular de los datos deberá dirigir a la Fundación una solicitud que contenga su nombre y apellidos y fotocopia de su DNI (o acreditación de su identidad por cualquier otro medio válido en derecho) o persona que lo representa, así como el documento acreditativo de tal representación; petición en que se concreta la solicitud; domicilio a efectos de notificaciones y fecha y firma del solicitante. Se recoge modelo de solicitud en el **Anexo XII** del presente Manual de Protección de Datos.

- En la solicitud, el interesado deberá indicar, además, si solicita la supresión total o parcial de sus datos personales. En este caso, deberá indicar los datos que solicita sean suprimidos.
- Si la solicitud no reúne los requisitos recogidos en los puntos anteriores, la Fundación debe solicitar su subsanación.
- La Fundación debe contestar la solicitud, utilizando cualquier medio que permita acreditar su envío y recepción.
- La solicitud deberá ser resuelta en el **plazo de un mes** a contar desde su recepción.
- Si la resolución fuera estimatoria, se debe proceder al bloqueo de los datos solicitados y pasado el plazo de prescripción de las posibles responsabilidades o acciones consecuencia del tratamiento de datos se debe proceder a su efectiva supresión. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación positiva al ejercicio de derechos.
- El ejercicio del derecho de supresión podrá ser denegado cuando ya se haya ejercitado este derecho en un intervalo inferior a **6 meses** y el interesado no acredite un interés legítimo o cuando pudiese causar un perjuicio a intereses legítimos, tanto del titular de los datos como de terceros; cuando exista una obligación legal que impida la supresión de los datos; el tratamiento sea necesario para ejercer el derecho a la libertad de expresión e información; por razones de interés público en el ámbito de la salud pública; para la formulación, el ejercicio o la defensa de reclamaciones; o por fines de archivo de interés público, de investigación científica o histórica, o estadísticos. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación negativa al ejercicio de derechos.
- En el caso de que no se dispongan de datos personales del interesado, se deberá igualmente comunicar en el mismo plazo.
- Se debe informar al interesado de su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD) o Autoridad de Control correspondiente, así como la posibilidad de ejercer ante el Responsable del Tratamiento cualquier otro derecho de protección de datos.
- En los casos en los que siendo procedente la supresión de los datos, no sea posible su eliminación, ya sea por razones técnicas o por causa del procedimiento o soporte utilizado, la Fundación procederá a su bloqueo para impedir su posterior tratamiento o utilización.
- En los casos en los que los datos objeto del ejercicio del derecho de supresión hayan sido comunicados a terceras personas y se mantenga el tratamiento por éstas, la

organización deberá comunicarles la supresión para que ellas también la efectúen, especialmente cuando dichos datos hayan sido hechos públicos y sea necesaria la supresión de cualquier enlace a los datos, así como cualquier copia o réplica de los mismos (derecho al olvido).

7.5. Derecho a la limitación del tratamiento

Los interesados pueden obtener de **FIBHULP** la limitación del tratamiento de sus datos si impugna la exactitud de los mismos, si el tratamiento es ilícito o innecesario o si se opone al tratamiento.

- Para ejercitar el derecho a la limitación del tratamiento, el titular de los datos deberá dirigir a la Fundación una solicitud que contenga su nombre y apellidos y fotocopia de su DNI (o acreditación de su identidad por cualquier otro medio válido en derecho) o persona que lo representa, así como el documento acreditativo de tal representación; petición en que se concreta la solicitud; domicilio a efectos de notificaciones y fecha y firma del solicitante. Se recoge modelo de solicitud en el **Anexo XII** del presente Manual de Protección de Datos.

- En la solicitud, el interesado deberá indicar, además, si solicita la limitación total o parcial de sus datos personales. En este caso, deberá indicar los datos sobre los que ejerce el derecho. Además, en caso de ser necesario, la solicitud requerirá la documentación que justifique la limitación del tratamiento.

- Si la solicitud no reúne los requisitos recogidos en los puntos anteriores, la Fundación debe solicitar su subsanación.

- La Fundación debe contestar la solicitud, utilizando cualquier medio que permita acreditar su envío y recepción.

- La solicitud deberá ser resuelta en el **plazo de un mes** a contar desde su recepción.

- Si la resolución fuera estimatoria, se debe proceder a la limitación del tratamiento de los datos solicitados. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación positiva al ejercicio de derechos. Cuando proceda el levantamiento de la limitación del tratamiento, se deberá informar al interesado previamente.

- El ejercicio del derecho a la limitación del tratamiento podrá ser denegado cuando ya se haya ejercitado este derecho en un intervalo inferior a **6 meses**, o si se ha verificado la exactitud de los datos, la licitud del tratamiento o la necesidad e interés legítimo del Responsable del Tratamiento, o si se considera que el interesado no necesita la

limitación del tratamiento de sus datos para la formulación, el ejercicio o la defensa de reclamaciones. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación negativa al ejercicio de derechos.

- En el caso de que no se dispongan de datos personales del interesado, se deberá igualmente comunicar en el mismo plazo.
- Se debe informar al interesado de su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD) o Autoridad de Control correspondiente, así como la posibilidad de ejercer ante el Responsable del Tratamiento cualquier otro derecho de protección de datos.
- En los casos en los que los datos objeto del ejercicio de este derecho hayan sido comunicados a terceras personas y se mantenga el tratamiento por éstas, la Fundación deberá comunicarles la limitación del tratamiento de los datos para que ellas también la efectúen.

7.6. Derecho a la portabilidad

Los interesados tienen derecho a recibir, por parte de **FIBHULP**, los datos personales que les incumban y que hayan facilitado al Responsable del Tratamiento, en un formato estructurado, de uso común y lectura mecánica; así como a transmitirlos, cuando sea técnicamente posible, a otro Responsable del Tratamiento, sin que lo impida el Responsable al que se los hubiera facilitado, siempre que el tratamiento esté basado en el consentimiento o en un contrato, y se efectúe por medios automatizados.

- Para ejercitar el derecho a la portabilidad, el titular de los datos deberá dirigir a la Fundación una solicitud que contenga su nombre y apellidos y fotocopia de su DNI (o acreditación de su identidad por cualquier otro medio válido en derecho) o persona que lo representa, así como el documento acreditativo de tal representación; petición en que se concreta la solicitud; domicilio a efectos de notificaciones y fecha y firma del solicitante. Se recoge modelo de solicitud en el **Anexo XII** del presente Manual de Protección de Datos.

- En la solicitud, el interesado deberá indicar si desea recibir los datos o transmitirlos directamente a otro Responsable del Tratamiento, si solicita la portabilidad total o parcial de sus datos personales. En este caso, deberá indicar los datos sobre los que ejerce el derecho.
- Si la solicitud no reúne los requisitos recogidos en los puntos anteriores, la Fundación debe solicitar su subsanación.

- La Fundación debe contestar la solicitud, utilizando cualquier medio que permita acreditar su envío y recepción.
- La solicitud deberá ser resuelta en el **plazo de un mes** a contar desde su recepción.
- Si la resolución fuera estimatoria, se debe proceder a la portabilidad de los datos solicitados. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación positiva al ejercicio de derechos.
- El ejercicio del derecho a la portabilidad podrá ser denegado cuando ya se haya ejercitado este derecho en un intervalo inferior a **6 meses** y el interesado no acredite un interés legítimo, o si puede afectar negativamente a los derechos y libertades de terceros, o si el tratamiento de los datos por parte del Responsable del Tratamiento no está basado en el consentimiento del interesado o en un contrato, o si dicho tratamiento no se efectúa por medios automatizados. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación negativa al ejercicio de derechos.
- En el caso de que no se dispongan de datos personales del interesado, se deberá igualmente comunicar en el mismo plazo.
- Se debe informar al interesado de su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD) o Autoridad de Control correspondiente, así como la posibilidad de ejercer ante el Responsable del Tratamiento cualquier otro derecho de protección de datos.

7.7. Derecho de oposición

Los interesados tienen derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de un tratamiento basado en el interés público o en el interés legítimo de **FIBHULP**, incluida la elaboración de perfiles sobre la base de dichos intereses.

- Para ejercitar el derecho de oposición, el titular de los datos deberá dirigir a la Fundación una solicitud que contenga su nombre y apellidos y fotocopia de su DNI (o acreditación de su identidad por cualquier otro medio válido en derecho) o persona que lo representa, así como el documento acreditativo de tal representación; petición en que se concreta la solicitud; domicilio a efectos de notificaciones y fecha y firma del solicitante. Se recoge modelo de solicitud en el **Anexo XII** del presente Manual de Protección de Datos.
- En la solicitud, el interesado deberá indicar, además, si se opone al tratamiento total o parcial de sus datos personales. En este caso, deberá indicar los datos sobre los que

ejerce el derecho. Además, en caso de ser necesario, la solicitud requerirá la documentación que justifique el ejercicio del derecho.

- Si la solicitud no reúne los requisitos recogidos en los puntos anteriores, la Fundación debe solicitar su subsanación.
- La Fundación debe contestar la solicitud, utilizando cualquier medio que permita acreditar su envío y recepción.
- La solicitud deberá ser resuelta en el **plazo de un mes** a contar desde su recepción.
- Si la resolución fuera estimatoria, el Responsable del Tratamiento interrumpirá el tratamiento de los datos solicitados. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación positiva al ejercicio de derechos.
- El ejercicio del derecho de oposición podrá ser denegado cuando ya se haya ejercitado este derecho en un intervalo inferior a **6 meses**, o si se acreditan motivos legítimos imperiosos por parte del Responsable del Tratamiento o si el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones. En el **Anexo XIII** del presente Manual de Protección de Datos se recoge el modelo de contestación negativa al ejercicio de derechos.
- En el caso de que no se dispongan de datos personales del interesado, se deberá igualmente comunicar en el mismo plazo.
- Si el solicitante manifiesta su deseo de no recibir comunicaciones comerciales, FIBHULP debe informarle sobre los sistemas de exclusión publicitaria existentes.

8. Anexos

ANEXO I: Registro de Actividades de Tratamiento

Las Actividades de Tratamiento de datos realizadas por **FIBHULP**, tanto como responsable del tratamiento como encargado del tratamiento, se encuentran recogidas en el archivo Excel "**RAT FIBHULP**".

ANEXO II: Relación de usuarios

La relación de usuarios con acceso al Sistema Operativo y a las aplicaciones necesarias para el tratamiento de los datos se encuentran recogidas, respectivamente, en el directorio activo y en el gestor de usuarios de las distintas aplicaciones.

No obstante, en el "**RAT FIBHULP**" se recoge una pestaña con la relación de usuarios con acceso autorizado a soportes o aplicaciones.

ANEXO III: Relación de prestaciones de servicios

La relación de prestaciones de servicios con acceso a datos personales o con libre acceso a las instalaciones del responsable del tratamiento se encuentra recogida en la pestaña correspondiente en el archivo Excel "**RAT FIBHULP**".

ANEXO IV: Registro de incidencias

En el archivo Excel "**Anexos MPD**" se recoge el Registro de incidencias y el Registro de recuperación de datos a utilizar en caso de producirse incidencias que afecten a datos personales.

ANEXO V: Inventario de soportes

En el archivo Excel "**Anexos MPD**" se recoge el inventario de soportes.

ANEXO VI: Registro de entrada y salida de soportes

En el archivo Excel "**Anexos MPD**" se recoge el registro de entrada y salida de soportes.

ANEXO VII: Registro de accesos

En el archivo Excel "**Anexos MPD**" se recoge el registro de accesos a documentación en soporte papel que contenga **datos sensibles**. Esta plantilla debe incorporarse a las carpetas o archivadores que almacenan estos soportes siempre que dos o más personas puedan acceder a los mismos.

Las aplicaciones que almacenan datos sensibles deben estar configuradas para registrar la identificación del usuario, la fecha y hora del acceso, a qué datos ha tenido acceso, el tipo de acceso, si ha sido denegado o permitido el acceso y, en este caso, información que permita identificar el registro accedido y qué acción ha realizado.

ANEXO VIII: Registro de controles periódicos

El Delegado de Protección de Datos (DPO), los Responsables Funcionales y el Responsable de Seguridad Técnico revisarán periódicamente el cumplimiento de los controles correspondientes, recogidos en el archivo Excel "**Anexos MPD**".

ANEXO IX: Delegación de autorizaciones

En la pestaña Delegación de autorizaciones del archivo Excel "**Anexos MPD**" se hace referencia a las funciones que los Responsables Funcionales, el Responsable de Seguridad Técnico Responsable Funcional, el Responsable de Seguridad Técnica o el Gestor de Solicitudes de Ejercicio de Derechos delegan a diferentes usuarios.

ANEXO X: Recibo del MPD por los empleados o usuarios

El modelo de recibo del MPD debe ser firmado por cada trabajador/usuario de **FIBHULP** que acceda a datos personales, como prueba de la recepción por el mismo del presente Manual de Protección de Datos de **FIBHULP**. Este modelo se encuentra recogido en el archivo "**Recibo del MPD**".

En el archivo Excel "**Anexos MPD**" se recoge una plantilla para controlar la recepción del presente Manual de Protección de Datos por parte de los Usuarios.

ANEXO XI: Solicitudes de ejercicios de derechos por el interesado

En el archivo Excel "**Anexos MPD**" se recoge la plantilla para controlar las solicitudes de ejercicio de derechos.

ANEXO XII: Modelos de solicitudes de ejercicios de derechos por el interesado

Los modelos de solicitudes para el ejercicio de derechos se encuentran recogidas en el archivo "**Modelos solicitud ejercicio de derechos**".

ANEXO XIII: Modelos de contestación o denegación al ejercicio de derechos por el interesado

Las plantillas de respuesta al ejercicio de derechos se encuentran recogidas en el archivo "**Modelos contestación ejercicio de derechos**".

ANEXO XIV: Nombramientos: DPO y Responsables

Las plantillas de Nombramientos de Responsables a firmar por las personas designadas se encuentran recogidas en el archivo "**Nombramientos RGPD**".

ANEXO XV: Cláusula Informativa - General

Cláusula informativa general

Le informamos que sus datos personales serán tratados por **FIBHULP** con la finalidad de _____.

Sus datos podrán ser cedidos a las entidades necesarias para realizar esta gestión: _____. Igualmente, sus datos podrán ser comunicados a diferentes prestadores de servicios de la empresa.

La base que legitima el tratamiento de sus datos personales es _____ y es imprescindible para llevar a cabo las gestiones indicadas. Así mismo, sus datos serán conservados _____, o durante los plazos de prescripción marcados por la ley.

Ud. puede ejercer sus derechos de acceso, rectificación, cancelación, oposición, portabilidad y limitación del tratamiento de sus datos dirigiéndose a FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO LA PAZ, a la dirección Paseo de la Castellana 261, 28046 de Madrid, o vía correo electrónico al email protecciondedatos@idipaz.es, acompañando copia de su DNI acreditando debidamente su identidad. En cualquier situación, Ud. tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

Datos Delegado de Protección de Datos (DPO) de FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO LA PAZ:

Alaro Avant, S.L.
dpo.fiblapaz@alaroavant.com

En Madrid, a .....de.....de 20..

Firma del interesado:

→ Las cláusulas elaboradas para cada una de los interesados se encuentran recopiladas en la carpeta "Cláusulas RGPD".

ANEXO XVI: Listado de prestadores de servicios

Los modelos de contratos de prestación de servicios se encuentran recopilados en la carpeta **"Contratos RGPD".**

ANEXO XVII: Gestión y Notificación de Brechas de Seguridad

El Procedimiento y las Plantillas para la Gestión y Notificación de Brechas de Seguridad se encuentran recogidas en el archivo "**Procedimiento Brechas de Seguridad**".

ANEXO XVIII: Formulario de Verificación

Los formularios de verificación para evaluar la necesidad de llevar a cabo una EIPD forman parte del archivo Excel que contiene los Registros de Actividades de Tratamiento de FIBHULP.

ANEXO XIX: Plazos orientativos de conservación de los datos

A continuación se recoge un listado de referencias legales a plazos de conservación de los datos. Este listado es meramente ilustrativo. FIBHULP debe estar al día de las normas que le son de aplicación en cada caso, normas que pueden recoger otros plazos de conservación diferentes a los de la siguiente tabla.

ACTIVIDAD DE TRATAMIENTO	DOCUMENTO	CONSERVACIÓN	ORIGEN DEL CRITERIO
Clientes	Facturas	10 años	Código Penal, Normativa contable, Código de Comercio, Normativa IVA, LIS
	Contratos	Con carácter general 5 años	Prescripción Código Civil
	Documentación a efectos del blanqueo de capitales y la financiación del terrorismo	10 años	Ley de lucha contra el blanqueo de dinero y la financiación del terrorismo
Recursos Humanos	Nóminas, TC1, TC2, etc.	10 años	Código Penal, Normativa contable, Normativa laboral, Código de Comercio, Normativa IVA, LIS
	Currículums	Hasta el fin del proceso de selección o 1 año	Recomendación
	Documentación indemnizaciones por despido	4 años	Ley de Infracciones y Sanciones en el Orden Social
	Contratos	4 años	Ley de Infracciones y Sanciones en el Orden Social
	Datos trabajadores temporales	4 años	Ley de Infracciones y Sanciones en el Orden Social

ACTIVIDAD DE TRATAMIENTO	DOCUMENTO	CONSERVACIÓN	ORIGEN DEL CRITERIO
	Expediente del trabajador	Hasta la baja y posteriormente durante un plazo de 5 años	Recomendación
Marketing	Bases de datos	Mientras dure el Tratamiento	Recomendación
	Visitantes web	Mientras dure el Tratamiento	Recomendación
Proveedores	Facturas	10 años	Código Penal, Normativa contable, Código de Comercio, Normativa IVA, LIS
	Contratos	Con carácter general 5 años	Prescripción Código Civil
Control de acceso y videovigilancia	Lista de visitantes	30 días	Instrucción de Control de Acceso a edificios
	Vídeos	A partir de 25 de mayo de 2018: 30 días destrucción, salvo incidente	Instrucción de Videovigilancia
Contabilidad	Libros y Documentos contables	6 años	Código de Comercio
	Acuerdos socios y consejos de administración, estatutos de la sociedad, actas, reglamento consejo de administración y comisiones delegadas	6 años	Código de Comercio
	Estados financieros, informes de auditoria	6 años	Código de Comercio
	Registros y documentos relacionados con subvenciones	6 años	Ley General de Subvenciones y Código de Comercio
Fiscal	Llevanza de la administración de la empresa, derechos y obligaciones relativos al pago de impuestos	10 años	Ley General Tributaria y Código Penal
	Información sobre el establecimiento de precios intragrupo	18 años; 8 años transacciones intragrupo para los acuerdos de precios	Ley Impuesto de Sociedades
	Administración de pagos de dividendos y retenciones fiscales	10 años	Ley General Tributaria
Seguridad y Salud	Prevención de Riesgos Laborales	5 años	Ley de Infracciones y Sanciones en el Orden Social
	Servicio Médico a Trabajadores	5 años (como mínimo)	Ley de Autonomía del Paciente (las leyes autonómicas pueden variar los plazos de conservación)
Medioambiente	Documentos relativos a permisos medioambientales	Mientras se lleve a cabo la actividad/ 3 años tras el cierre de la actividad	Ley 16/2002 (modificada por la Ley 5/2013) y Código Penal
		10 años (prescripción delito)	
	Registros sobre reciclaje o la eliminación de residuos	3 años	Ley 22/2011 de residuos y suelos contaminados
	Responsabilidad medioambiental	3 años	Ley 26/2007 de Responsabilidad Medioambiental

ACTIVIDAD DE TRATAMIENTO	DOCUMENTO	CONSERVACIÓN	ORIGEN DEL CRITERIO
Seguros	Pólizas de seguros	6 años (regla general)	Código de Comercio, Ley de Contrato de Seguro, Ley de lucha contra el blanqueo de dinero y la financiación del terrorismo y Código Civil.
		2 años (seguro de daños) 5 años (seguros personales) 10 años (seguro de vida)	
Jurídico	Documentos Propiedad Intelectual e Industrial	5 años	Ley de Patentes, Ley de Marcas, Ley de Propiedad Intelectual, Ley de Protección Jurídica del Diseño
	Contratos y acuerdos	5 años con carácter general	Prescripción Código Civil
	Permisos, licencias, certificados	6 años desde la fecha de expiración del permiso, licencia, certificado 10 años (prescripción penal)	Código de Comercio
	Acuerdos de confidencialidad y de no competencia	Siempre o plazo de duración obligación confidencialidad	Recomendación

ANEXO XX: Evaluación de Impacto relativa a la Protección de Datos

El Procedimiento y las Plantillas para llevar a cabo una Evaluación de Impacto relativa a la Protección de Datos (EIPD) se encuentran recogidas en el archivo "Procedimiento EIPD".

ANEXO XXI: Política Interna de Garantía de los Derechos Digitales

La Política Interna de Garantía de los Derechos Digitales se encuentra recogida en el archivo "Política Interna – Derechos Digitales".

En la elaboración de esta Política Interna de Garantía de los Derechos Digitales deberán participar los representantes de los trabajadores, si es el caso.

La entidad deberá incluir en esta Política únicamente aquellas medidas que haya implantado relativas a videovigilancia, grabación de sonidos, huella digital y geolocalización

Esta Política debe ser firmada por la entidad y por el trabajador.